

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 <^{NR.}> direkt angesteuert werden.
- ✓ Integrierte Monatsinformationen: Januar bis Dezember 2025

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



(Einfach interessantes Thema nach Wahl anklicken)

1. Standard – Datenschutz – Modell Vers. 3.1a	1
a) Update Standard-Datenschutz-Modell (SDM)	5
2. Zum Datenschutz	5
a) Löschkonzept erstellt?	5
(1) In der DS-GVO dazu:	5
(2) Mögliche Antworten des Verantwortlichen u/o Datenschutzbeauftragten	5
(3) Löschkonzept (Inhalte)	5
b) Wie weit geht das Auskunftsrecht?	5
(1) Hintergrund:	5
(2) Die Urteile:	6
(3) Welche möglichen Ausnahmen bestehen?	6
c) Doctolib – Gesundheitsdaten für KI-Modelle ???	6
d) Datenschutzverletzung und Meldepflichten	7
(1) Die Meldepflicht	7
(2) Die Datenschutzverletzung	7
(3) Handlungsempfehlungen	7
(3.1) Checkliste:	7
(3.2) Risikobegrenzung / -vermeidung:	8
e) Das Kopplungsverbot im Datenschutz	8
(1) Regelung in der DSGVO	8
(1.1) PS: UWG § 33 mit Anhang	8
(1.2) PS: GWB Kapitel 2 (§§ 18-21)	8
(2) Bedingungen der Aufsicht	8
f) Konflikt: Löschpflicht vs. Nachweispflicht?	9
g) Vorsicht für beide Seiten zum berechtigten Interesse des Verantwortlichen!	9
(1) DS-GVO	9
(2) Das 3-Stufen-Modell der EDSA	9
(2.1) Stufe 1 „Das Interesse an“	9
(2.2) Stufe 2 „Die Erforderlichkeitsprüfung“	9
(2.3) „Die Abwägungsprüfung“	9
(3) Praxisbeispiel: Die Meta-KI	10
(3.1) Stufe 1 berechtigtes Interesse: „Zu vage!“	10
(3.2) Stufe 2 Erforderlichkeit: „Unspezifisch!“	10
(3.3) Stufe 3 Abwägung: „Mangelhaft!“	10
(4) Eine Empfehlung:	10
h) Pseudonymisierung	10
(1) Der Begriff kurz erklärt:	10
(2) In der DSGVO (Art. 4 Nr. 5):	10
(3) Warum Pseudonymisierung:	11
(4) Beispiel:	11
(4.1) Hintergrund:	11
(4.2) Ziel:	11
(4.3) Eine Lösung:	11



i) Öffentlich zugängliche Daten und Werbung.....	11
j) Datenverarbeitung des Betriebsarztes.....	11
k) Hinweis zum Datentransfer mit den USA.....	12
l) Künstliche Intelligenz (KI oder AI) und der Datenschutz.....	13
(1) Die vorderen Plätze:.....	13
(2) Die hinteren Plätze:.....	13
(3) Beispiel: Datenschutzrisiken von Microsoft 365 Copilot.....	13
(4) KI-Trainingsdaten mit personenbezogenen Inhalten gefunden.....	14
m) Einsatz von KI im Unternehmen.....	14
(1) Fazit einer Studie:.....	14
(2) Die bessere, europäische Antwort zu KI.....	14
(2.1) Wer ist Mistral.....	14
(2.2) Was ist Mistral.....	14
(2.3) Datenschutz statt Datenklau.....	14
n) Mein Datenschutzstatus schnell ermittelt.....	15
o) Nicht jeder darf „Datenschutzbeauftragter“.....	15
(1) Wenn, wann?.....	15
(2) Wenn, wen?.....	15
(3) Wenn, wen nicht!.....	15
p) Automatische Webseitenprüfung der Aufsicht.....	16
q) „Viel zu klein für eine Prüfung der Datenschutzaufsicht?“.....	16
(1) Auslöser:.....	16
(2) Einfache (Bußgeld) Gründe dafür.....	16
r) Gültigkeit der Einwilligung.....	17
(1) Z. B. Talentpool mit Bewerberdaten.....	17
(2) Z. B. Website mit Mitarbeiterfotos.....	17
(3) Empfehlung:.....	17
s) Immer wieder E-Mail.....	18
(1) Anlass:.....	18
(2) Datenschutzsicht:.....	18
(3) Empfehlung:.....	19
3. Zur Datensicherheit.....	19
a) DMA, DORA, DSA, KRITIS, CERT & NIS-2?.....	19
(1) DMA – Digital-Markets-Act.....	19
(2) DSA – Digital-Service-Act.....	19
(3) DORA – Digital-Operational-Resilience-Act.....	19
(4) NIS-2 (Network-and-Information-Security).....	20
(5) KRITIS – Kritische Infrastruktur (CER).....	20
b) Manipulierte Rechnung per E-Mail.....	20
(1) Der Fall.....	20
(2) Das Urteil.....	20
c) HP-Universal-Drucker-Treiber mit kritischer Sicherheitslücke (UPDATE !!!).....	20
d) Sicherheitslücken – Risiko für die Guten.....	21

e) BSI empfiehlt den Wechsel von Windows 10.....	21
f) BSI, KI und Captchas.....	21
g) Identitätsdiebstahl.....	21
h) Kündigung wegen Datenschutzverletzung.....	22
i) E-Mails, ohne geht es nicht, aber ...!	22
(1)  <i>Bedrohungsszenarien</i>	22
(2)  <i>Schutzmaßnahmen</i>	22
(3)  <i>Empfehlungen für Organisationen</i>	22
j) BSI zu KI Systemen.....	22
k) Verschnaufpause Windows 10.....	23
l) Sicherheitshinweis für Microsoft Teams.....	23
m) Bremsen Datenschutzvorschriften die KI aus, oder helfen sie sogar?.....	23
n) Handy – Richtlinie der NSA.....	23
o) Erfasst MS-Teams die Büroanwesenheit?.....	23
p) Sichere -E-Mail Verschlüsselung und ein Problem davor.....	24
(1) <i>Funktionsweise:</i>	24
(2) <i>Einfaches Beispiel:</i>	24
(3) <i>Und das Problem ist?</i>	24
(4) <i>Hinweis:</i>	25
4. Zu angrenzenden Themen.....	25
a) Hält der EU US-Angemessenheitsbeschluss?.....	25
b) Die „Dracula Suite“.....	25
c) GoBD Änderung Fristen.....	25
d) ☐ Supportende Windows 10.....	25
e) Keine Werbung!.....	25
f) Abschaltung US-basierender Digitaldienste durch US-Regierung?.....	26
g) Praktische KI (AI).....	26
h) KI aus Europa?.....	26
i) Mal einen Blick auf Geldbußen für DSGVO-Verstöße in Deutschland 2025.....	26
(1) € 45 Mio. „unzureichend“.....	26
(2) € 120.000 „verspätet“.....	26
(3) € 30.000 „unerlaubt“.....	26
j) Paypal aber sicher.....	26
k) Dringliche Sicherheitswarnung von Samsung wegen WhatsApp.....	26
l) Nützliche Informationen – verständlich!.....	27
m) „Ich bin doch uninteressant für Hacker, oder?“.....	27
(1) <i>Kompromittierungsmethoden:</i>	27
(2) <i>Schutzmethoden</i>	27
n) Europäische Suchmaschine(n).....	28

a) Update Standard-Datenschutz-Modell (SDM)

Das SDM erhielt eine kleine Auffrischung von Version 3.1 auf 3.1a, mit neuem Logo und neuer Abbildungen(3, 4, 5) zum Kapitel D2.6 Überblick über die Modellierungstechniken des SDM („SDM-Würfel“ Seite 44ff). Die Art der Maßnahmenkataloge (Bausteine zum SDM) wird überarbeitet und ist in Arbeit um konkretere (bessere Praxisnähe) Bezüge zum SDM herzustellen.

2. Zum Datenschutz

a) Löschkonzept erstellt?

„Haben wir ein Löschkonzept?“ – „Wer will das wissen?“ – „Ein (Geschäfts-) Kunde!“

(1) In der DS-GVO dazu:

In Verbindung mit der Rechtmäßigkeit der Verarbeitung nach [Art.6 DS-GVO](#) (Einwilligung, Vertragsanbahnung und -erfüllung, gesetzliche Vorgaben oder im Interesse des Betroffenen und/oder des Verantwortlichen u. m.), dem [Art.17 DS-GVO](#) mit dem Recht auf Löschung („Recht auf Vergessenwerden“) ist in [Art.5 Abs.\(2\) DS-GVO](#) Grundsätze für die Verarbeitung personenbezogener Daten festgehalten:

„(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können ("Rechenschaftspflicht)"“

(2) Mögliche Antworten des Verantwortlichen u/o Datenschutzbeauftragten

- (a) „Ja, wir haben im Verzeichnis der Verarbeitungstätigkeiten zu allen erhobenen Daten bzw. Datenkategorien u. a. die Dauer der Verarbeitung und die Löschfristen festgehalten.“
- (b) „Ja, aus dem Verzeichnis der Verarbeitungstätigkeiten sind die Löschfristen in unser IT-Konzept eingeflossen“ (meist bei größeren IT-Strukturen).“
- (c) „Ja, aber nicht korrekt dokumentiert.“

(3) Löschkonzept (Inhalte)

Sofern im Verzeichnis der Verarbeitungstätigkeiten die Löschfristen und deren Umsetzung in den technisch-organisatorischen Maßnahmen nicht festgehalten sind (**Antwort (c)**), sollte ein Löschkonzept folgendes beinhalten (oder diese im VVT ergänzt werden):

- (a) **Zielsetzung** (Einhaltung der DS-GVO Daten zu löschen, wenn diese nicht mehr erforderlich sind und dabei gesetzliche Aufbewahrungsfristen und technische Standards einzuhalten)
- (b) **Geltungsbereich** (z. B. Die gesamte Organisation einschl. aller zugehörigen Einheiten)
- (c) **Verantwortlichkeiten** (Einheit, Abteilung, IT-Abteilung und Überwachung durch DSB)
- (d) **Datenklassifizierung** (Einteilung nach Aufbewahrungsfristen und Risikokategorien)
- (e) **Technisch-organisatorische Maßnahmen** (Sicherstellung zur Einhaltung der Fristen)
- (f) **Überprüfungen & Anpassung** (Einhaltung der Maßnahmen und der Dokumentation)

b) Wie weit geht das Auskunftsrecht?

Schon der Titel der Pressemitteilung 20/2024 des Oberlandesgerichts Oldenburg¹ klingt nicht uninteressant:

„Zwischen Detektiveinsatz und Datenschutz – Anspruch auf Offenlegung eines Detektivberichts nach geheimer Observation durch die Versicherung?“

(1) Hintergrund:

Im Rahmen eines Unfallversicherungsschadens hat die Versicherung des Unfallverursachers eine Detektei beauftragt, die Korrektheit der Angaben zur Verletzung des Unfallopfers zu beobachten. Die mehrwöchigen Beobachtungen über die gesundheitlichen Alltagseinschränkungen hat die Detektei in einem Bericht zusammengefasst und der Versicherung übergeben.

Eine Auskunftsanfrage nach Art.15 DSGVO hat die Versicherung zwar beantwortet, aber ohne den Bericht der Detektei beizufügen. Deren Offenlegung würde ihren Verteidigungsinteressen schaden.

¹ Quelle: Niedersachsen / Oberlandesgericht Oldenburg: „Zwischen Detektiveinsatz und Datenschutz ...“
Dokument von <https://volkerschroer.de>

(2) Die Urteile:

Das Landgericht hatte der Versicherung ein überwiegendes Geheimhaltungsinteresse zuerkannt und die Klagen abgewiesen und:

„Das Oberlandesgericht Oldenburg verurteilte die Versicherung zur Auskunft über die personenbezogenen Daten des Klägers und zur Herausgabe einer Kopie des Observationsberichts der Detektei. Der Senat stellte fest, dass dem Kläger ein Auskunftsanspruch nach der Datenschutzgrundverordnung (Art. 15 DSGVO) zustehe, da vom Kläger personenbezogene Daten gesammelt und verarbeitet worden seien. Betroffenen stünde in solchen Fällen ein generell schutzwürdiges Interesse an der Auskunft zu. Denn das Auskunftsrecht verfolgte gerade den Zweck, sich der Verarbeitung der personenbezogenen Daten bewusst zu werden und deren Rechtmäßigkeit zu überprüfen. Grundsätzlich könne der Auskunftsanspruch zwar durch Rechte anderer Personen eingeschränkt sein. Ein solches Gegenrecht habe die Versicherung in diesem Fall aber nicht darlegen können.“

(3) Welche möglichen Ausnahmen bestehen?

Da wäre zunächst der § 34 des Bundesdatenschutzgesetzes, bei Datenverarbeitung zu wissenschaftlichen, historischen Forschungs- und Statistikzwecken, im öffentlichen Interesse liegenden Archivzwecken, aufsichtsbehördlichen Befugnissen im Fall von Geheimhaltungsinteressen, Daten, die nur aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen und Datenverarbeitungen, die ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen und die Auskunftserteilung einen unverhältnismäßig hohen Aufwand erfordert (Beispiel sind hier die 48-Stunden-Videoaufnahmen in Bus und Bahn, die automatisch gelöscht werden, sofern kein Vorfall eingetreten ist.). Natürlich ist eine Auskunftsverweigerung zu dokumentieren!

Dann gibt es da noch die gewerblichen Schutzrechte², darunter Patent, Gebrauchsmuster, Design, Marke, sowie Urhebergesetz und Nachahmungsschutz durch Wettbewerbsrecht.

Eine Auskunftsbeschränkung könnte noch nach dem Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) geltend gemacht werden. Nach § 2 GeschGehG sind Geschäftsgeheimnisse nicht allgemein bekannt, nicht ohne Weiteres zugänglich und daher von wirtschaftlichem Interesse. Durch den Inhaber (natürliche oder juristische Person) mit angemessenen Maßnahmen geschützt und damit ein berechtigtes Interesse an der Geheimhaltung besteht.

c) Doctolib – Gesundheitsdaten für KI-Modelle ???

Wie NETZPOLITIK.ORG berichtet³, hat der IT-Dienstleister Doctolib seine Datenschutzhinweise aktualisiert. Als grenzwertig anzusehen ist das „berechtigte Interesse“ (also ohne vorherige Zustimmung der Nutzer) an Daten zu Geschlecht, Geburtsmonat, -jahr und von freiwilligen Antworten auf Umfragen. Bei der Verwendung weiterer Gesundheitsdaten darf der Nutzer entscheiden, bzw. seine informierte, freiwillige und unbeeinflusste Einwilligung erteilen. Abgesehen von Patientenbeschwerden über Praxen, die ausschließlich Termine über Doctolib ermöglichen und einer Recherche von mobilsicher.de über die zeitweise übertragenen, sensiblen Gesundheitsdaten an Facebook und die Werbepattform Outbrain, stört mich schon der Punkt 4.2 in den Datenschutzbestimmungen⁴:

4.2. Personenbezogene Daten, die aus öffentlichen Quellen oder von Dritten erhoben werden

Doctolib kann Ihre personenbezogenen Daten von Dritten erhalten. Gesundheitsfachkräfte: Gesundheitsfachkräfte können bei der Nutzung der Doctolib-Dienste Ihre personenbezogenen Daten in die Plattform eingeben, unabhängig davon, ob Sie ein Doctolib-Nutzerkonto erstellt haben. In diesem Fall erhebt Doctolib Ihre personenbezogenen Daten von den Gesundheitsfachkräften. Nutzer können in ihrem Nutzerkonto Angehörige anlegen. In diesem Fall – wenn Sie ein Angehöriger sind – werden Ihre personenbezogenen Daten von diesen Nutzern erhoben.

Auf eine schon länger zurückliegende Auskunftsanfrage hat mir Doctolib mitgeteilt, dass sie nur Auftragsverarbeiter sind, da ich kein Nutzerkonto angelegt hätte. Die Anfrage ist in diesem Fall an den Verantwortlichen nach DSGVO, den Arzt bzw. die Praxis zu richten. Zu diesem Zeitpunkt

² Quelle: Gabler Wirtschaftslexikon: „gewerbliche Schutzrechte“

³ Quelle: Netzpolitik.org: „Neue Datenschutzhinweise Doctolib will KI-Modelle mit Gesundheitsdaten trainieren“

⁴ Link: Doctolib: „Datenschutzhinweise (PDF)“

wurde das Tool in der Praxis nicht genutzt. Was dabei alles an Daten verarbeitet wird, ist in den Datenschutzhinweisen ab Punkt 6. nachzulesen.

Meine Abwägung: Auch wenn auf der Webseite Zertifizierungen zum Datenschutz durch TÜV Saarland, TÜVIT (TÜV-Nord-Gruppe) und ein BSI-C5 Zertifizierung durch einen Wirtschaftsprüfer (nicht vom, sondern nur nach BSI) aufgeführt sind, erschreckt mich der Umfang der Datenspeicherung laut Datenschutzhinweise auch ohne angelegtes Nutzerkonto ab. Und mit Zustimmung sollen zum Beispiel auch Informationen aus dem (für mich) vertraulichen 4-Augen-Gespräch des Patienten mit dem Arzt verarbeitet werden.

d) Datenschutzverletzung und Meldepflichten

(1) Die Meldepflicht

Nach [Art.33 Abs.1 DSGVO](#) ist im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich, innerhalb von 72 Stunden nachdem die Verletzung bekannt wurde, die zuständige Aufsichtsbehörde zu informieren. Dies gilt für Verantwortliche wie Auftragsverarbeiter. Es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der natürlichen Person führt.

(2) Die Datenschutzverletzung

Die Datenschutzverletzung ist in [Art.4 Nr.12 DSGVO](#) definiert.

"Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

Ein Verstoß gegen die DSGVO durch z. B. mangelnde Löschung, unrechtmäßige Datenverarbeitung oder mangelhaftes Verzeichnis der Verarbeitungstätigkeiten, wird im Falle einer Prüfung durch die Aufsichtsbehörde je nach der Schwere bemängelt und sanktioniert. Nach der Definition stellen diese Punkte bis dahin noch keinen Verlust, keine Veränderung, keinen unbefugten Zugriff und damit keine Datenschutzverletzung dar. Wird eine Veranstaltungseinladung ersichtlich an alle Teilnehmer („An“) gesendet und nicht an jede Person separat, dann handelt es sich um eine unbefugte Offenlegung und damit um eine Datenschutzverletzung. Hat ein unbefugter Dateneinblick über einen ungeschützten Desktop / Notebook oder eine offen liegende Personalakte, ist dies ebenfalls eine Datenschutzverletzung.

(3) Handlungsempfehlungen

Vorab: Verstöße gegen die Datenschutz-Grundverordnung sollte natürlich auch umgehend abgestellt werden. In allen Fällen sind auch die technisch-organisatorischen Maßnahmen (TOM) zu überprüfen und anzupassen (keine Frage)!

(3.1) Checkliste:

- ☐ Handelt es sich um einen Verstoß gegen die DSGVO ohne Beteiligung / Zugriff eines Dritten?
 - Fehler abstellen / TOM überprüfen und ggf. anpassen (!!!).
- ☐ Handelt es sich um den Verlust, die Vernichtung, die Veränderung, die unbefugte Offenlegung oder einen unbefugten Zugang von übermittelten, gespeicherten oder anderweitig verarbeiteten personenbezogenen Daten?
 - Nein. Fehler abstellen / TOM überprüfen und ggf. anpassen (!!!).
 - Ja, dann ist es eine Datenschutzverletzung und weiter mit dem nächsten Punkt!
- ☐ Führt die Datenschutzverletzung zu einem Risiko für die Rechte und Freiheiten der natürlichen Person?
 - Nein. Fehler abstellen / TOM überprüfen und ggf. anpassen (!!!).
 - Ja, die Maßnahmen und die Meldung an die Aufsichtsbehörde nach [Art.33 DSGVO](#) ist zwingend innerhalb von 72 Stunden nach Bekanntwerden vorzunehmen.

(3.2) Risikobegrenzung / -vermeidung:

Ein offener Umgang mit einer direkten Ansprache gegenüber dem/den Betroffenen ist der beste Weg, weil:

- ✓ Es besteht eine unverzügliche Informationspflicht im Falle einer Datenschutzverletzung gegenüber dem Betroffenen nach [Art.34 DSGVO](#) bei einem voraussichtlich hohen Risiko.
- ✓ Es kann eine sofortige Klärung des bestehenden Risikos für und mit dem Betroffenen vorgenommen werden („Sehen Sie ein Problem darin?“). Das schafft Vertrauen, und die Meldepflicht könnte entfallen, wenn der Betroffene darin kein Risiko sieht. Im gegenteiligen Fall können mit dem Betroffenen gleich Maßnahmen zur Behebung oder Abmilderung des Risikos getroffen werden.
- ✓ Nach [Art.33 Abs.3 d\)](#) ist die Meldung an die Aufsichtsbehörde, um eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Begrenzung und / oder Behebung zu dokumentieren.
- ✓ Die Erkenntnisse können zur Anpassung der technisch-organisatorischen Maßnahmen genutzt werden, um Vorfälle dieser Art künftig zu vermeiden.

e) Das Kopplungsverbot im Datenschutz

(1) Regelung in der DSGVO

Das Kopplungsverbot ist in [Art.7 Abs.4 DSGVO](#) Bedingungen für die Einwilligung geregelt und besagt:

„Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.“

Beim Surfen im Netz ist mir zum Kopplungsverbot neben der DSGVO noch aufgefallen:

(1.1) PS: UWG § 33 mit Anhang⁵

Daneben lohnt sich auch ein Blick in das Gesetz gegen den unlauteren Wettbewerb in § 3, zum Verbot unlauterer geschäftlicher Handlungen. Im Anhang zu § 3 sind grundsätzlich verbotene und irreführende Geschäfte aufgeführt, u. a. unwahre Angaben, unklare Lockangebote, als Information getarnte Werbung u. v. m.

(1.2) PS: GWB Kapitel 2 (§§ 18-21)⁶

Das Kopplungsverbot untersagt marktbeherrschenden Unternehmen, den Verkauf eines Produkts oder einer Dienstleistung an die Bedingung zu knüpfen, dass der Kunde ein anderes Produkt oder eine andere Dienstleistung mitkauft. Dieses Verhalten kann den Wettbewerb verzerren und den Marktzugang für Konkurrenten erschweren.

(2) Bedingungen der Aufsicht

Die Landesbeauftragte für den Datenschutz und die Informationsfreiheit NRW schreibt in ihrem 29. Bericht auf Seite 39ff⁷, dass die Nachverfolgung von Nutzern (Tracking) grundsätzlich auf eine Einwilligung gestützt werden kann, wenn alternativ ein trackingfreies Modell angeboten wird, selbst wenn dieses bezahlpflichtig ist. Damit kann auch ein „Ablehnen-Button“ vermieden werden, wenn:

- Für jeden Verarbeitungszweck oder zumindest für zusammengefasste, ähnliche Zwecke ist eine Einwilligung einzuholen (granulare Einwilligungen).
- Gebündelte Zwecke müssen einander ähnlich sein und dürfen nur eine überschaubare Anzahl von Zwecken enthalten.
- Da verlangte Entgelt muss marktüblich sein und einen gleichwertigen Zugang ermöglichen.
- Die Leistung, die Nutzende bei einem Bezahlmodell erhalten, müsse jedoch erstens eine

⁵ Quelle: [dejure.org](#): „[UWG §3 Verbot unlauterer geschäftlicher Handlungen](#)“

⁶ Quelle: Bundesamt für Justiz: „[Gesetz gegen Wettbewerbsbeschränkungen](#)“

⁷ Quelle: „[Pur-Abos im Internet können zulässig sein, müssen aber bestimmte Bedingungen einhalten.](#)“

gleichwertige Alternative zu der Leistung darstellen, die diese durch eine Einwilligung erlangen. Zweitens müsse die Einwilligung alle in der Datenschutz-Grundverordnung (DS-GVO) normierten Wirksamkeitsvoraussetzungen erfüllen.⁸

f) **Konflikt: Löschpflicht vs. Nachweispflicht?**

„Wenn man alle personenbezogene Daten löschen muss, fehlt nicht dann der Nachweis der berechtigten Verarbeitung der Daten (Rechtsgründe wie Einwilligung, vertragliche Gründe u.s.w.)?“

Fundstelle dazu ist der Jahresbericht 2023 der Berliner Beauftragten für Datenschutz und Informationsfreiheit⁹ auf der Seite 83 (bzw. Nr. 81). Antwort: „Nein, kein Konflikt“ Zitat:

„Ein Lösungsersuchen verpflichtet Verantwortliche nicht dazu, etwaige Nachweise für eine erteilte Einwilligung oder für das Vorliegen einer anderen Rechtsgrundlage zu löschen. Bei der Speicherung des Nachweises handelt es sich um einen eigenständigen Verarbeitungszweck. Verantwortliche sind nach der DSGVO verpflichtet, die Rechtmäßigkeit einer Verarbeitung nachweisen zu können. Können sie den Nachweis nicht erbringen, müssen sie damit rechnen, dass ein datenschutzrechtlicher Verstoß festgestellt wird.“

g) **Vorsicht für beide Seiten zum berechtigten Interesse des Verantwortlichen!**

(1) **DS-GVO**

Jede Verarbeitung von personenbezogenen Daten bedarf eines Rechtsgrundes nach [Art.6 DSGVO](#) und in Abs.1f) besagt (Zitat):

„die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.“

Danach ist eine Interessenabwägung zwischen den berechtigten Interessen des Verantwortlichen (der Unternehmung) und den Interessen der betroffenen Personen vorzunehmen. Wie geht das jetzt?

(2) **Das 3-Stufen-Modell der EDSA**

Der europäische Datenschutzausschuss (EDSA) zur Verarbeitung von personenbezogenen Daten im Zusammenhang mit KI-Modellen dazu eine Stellungnahme 28/2024¹⁰ veröffentlicht. Ab Seite 25ff wird zu den „Erwägungen in Bezug auf die dreistufige Prüfung der berechtigten Interessen“ ausgeführt.

(2.1) **Stufe 1 „Das Interesse an“**

Auf der ersten Stufe muss geprüft werden, ob der Verantwortliche (z. B. das Unternehmen) oder ein Dritter ein berechtigtes Interesse an der Datenverarbeitung hat. Das kann auch ein wirtschaftliches Interesse sein.

(2.2) **Stufe 2 „Die Erforderlichkeitsprüfung“**

Auf der zweiten Stufe ist dann zu prüfen, ob die begehrte Datenverarbeitung auch erforderlich ist, um die zuvor festgestellten Interessen zu wahren. Der Datenschutzausschuss betont, dass die Erforderlichkeit restriktiv auszulegen sei. Die Datenverarbeitung müsse auf „das unbedingt Notwendige“ beschränkt sein.

(2.3) **„Die Abwägungsprüfung“**

Auf der dritten Stufe ist dann die eigentliche Abwägung mit ggf. entgegenstehenden, überwiegenden Interessen der betroffenen Person durchzuführen. Je genauer ein Interesse im Hinblick auf den vorgesehenen Zweck der Verarbeitung definiert ist, desto besser wird es möglich sein, die

⁸ Quelle: DSK Datenschutzkonferenz des Bundes und der Länder: „[Bewertung von Pur-Abo-Modellen auf Websites](#)“

⁹ Quelle: Berliner Beauftragte für Datenschutz und Informationsfreiheit: „[Jahresbericht 2023 Datenschutz und Informationsfreiheit.pdf](#)“

¹⁰ Quelle: EDSA: „[Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen](#)“

tatsächlichen Gegebenheiten in Bezug auf die für die Abwägung zu berücksichtigenden Nutzen und Risiken klar zu verstehen. Bei den betroffenen Personen hat die Abwägung der Interessen gegen die Charta der Grundrechte der Europäischen Union (EU-Charta) zu erfolgen, z. B. das Recht auf Achtung des Privat- und Familienlebens (Artikel 7 EU-Charta) und das Recht auf den Schutz personenbezogener Daten (Artikel 8 EU-Charta).

(3) Praxisbeispiel: Die Meta-KI

Der „datenschutzticker.de“ hat die aktuelle Diskussion um den Einsatz der KI des Meta-Konzerns sehr gut und übersichtlich zusammengetragen¹¹. Nachfolgend in aller Kürze:

(3.1) Stufe 1 berechtigtes Interesse: „Zu vage!“

Die „Verbesserung der KI speziell auf europäische Nutzer“ – wird als zu vage kritisiert.

(3.2) Stufe 2 Erforderlichkeit: „Unspezifisch!“

Die fehlende Prüfung milderer Mittel wie Anonymisierung sowie eine unklare Eingrenzung der betroffenen Datenkategorien, insbesondere im Hinblick auf Art. 9 DSGVO wirft hier Zweifel auf.

(3.3) Stufe 3 Abwägung: „Mangelhaft!“

Das Opt-Out-Verfahren, das eine Begründung erfordert und im Ermessen von Meta liegt, deutet auf eine mangelnde Berücksichtigung der Nutzererwartungen hin. Der vorgesehene Widerspruchsmechanismus ist nutzerunfreundlich und unzureichend. Zudem fehlt es an einer echten Wahlmöglichkeit – etwa durch eine Einwilligung.

(4) Eine Empfehlung:

Es geht um Vertrauen, und Vertrauen schafft man nur mit Transparenz. Welche Daten werden für welchen Zweck erhoben, und besteht ggf. Einfluss auf die verarbeiteten Daten, um Schaden abwenden zu können. Das wird die Bereitschaft zur Unterstützung von KI-Trainingsmodellen und dem Einsatz von KI deutlich steigern. Zitat:

„Die Betonung von Transparenz, Datenminimierung und der Berücksichtigung der vernünftigen Erwartungen der Nutzer sind entscheidend, um das Vertrauen der Bürgerinnen und Bürger in KI-Technologien zu stärken“

h) Pseudonymisierung

Der europäische Datenschutzausschuss (EDSA) veröffentlichte die Leitlinien 01/2025 zur Pseudonymisierung und zusätzlich eine interessante Zusammenfassung, wann und wie Pseudonymisierung angewendet werden kann.¹² Die Vorlage beinhaltet 10 verständliche Beispiele für eine Umsetzung der Pseudonymisierung von personenbezogenen Daten. Also klassische Anwendungsfälle aus der Praxis, ohne hier allerdings eine präzise Rechtsgrundlage der einzelnen Konzepte zu benennen und eine Pflicht besteht auch nicht. Es kann aber bei der Festlegung der technisch-organisatorischen Maßnahmen sehr hilfreich sein.

(1) Der Begriff kurz erklärt:

Anonymisierte Daten sind nicht mehr mit der Person in Verbindung zu bringen und unterliegen nicht mehr dem Datenschutz. Pseudonymisierte Daten können nur über zusätzliche Angaben aus einer separaten, gesicherten Datei einer Person zugeordnet werden. Die Pseudonymisierung bietet mehrere Vorteile, darunter die Reduzierung von Sicherheitsrisiken und der Gefahr, Daten für einen nicht vereinbarten Zweck zu verwenden. Sie kann es Unternehmen zudem erleichtern, berechtigte Interessen als Rechtsgrundlage für die Datenverarbeitung heranzuziehen.

(2) In der DSGVO (Art. 4 Nr. 5):

"Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen

¹¹ Quelle: datenschutzticker.de: „Meta vs. DSGVO: Erlaubt der EDPB-3-Stufen-Test KI-Training mit Nutzerdaten?“

¹² Quelle: EDSA: „Guidelines 01/2025 on Pseudonymisation“

werden.

(3) Warum Pseudonymisierung:

Die Verarbeitung von personenbezogener Daten nach den Regeln des Datenschutzes ([Art.5 DSGVO](#)) lässt sich auf die verkürzte Formel reduzieren: „So wenige personenbezogene Daten wie möglich zu verarbeiten, aber nur so viele wie unbedingt nötig in einer Form, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke erforderlich ist durch geeignete technische und organisatorische Maßnahmen.“

Erhöhte „Technikgestaltung“ gilt es bei besonderen Kategorien von personenbezogenen Daten ([Art.9 DSGVO](#)), Kindern ([Art.8 DSGVO](#)) und strafrechtlich Verurteilungen und Straftaten ([Art.10 DSGVO](#)) einzuhalten. Die Pseudonymisierung ist eine in der DSGVO geregelte Maßnahme, die unter anderem das Ziel verfolgt, die Risiken für die betroffene Person zu verringern.

(4) Beispiel:

Das Beispiel stammt aus der Zusammenfassung (Summary) der EDSA zu den Leitlinien 01/2025.

(4.1) Hintergrund:

Das Unternehmen bietet eine Gesundheitsapp an, die medizinische Ratschläge basierend auf den Angaben des Nutzers zu Symptomen vorschlägt. Eine Abteilung ist für die Qualitätskontrolle verantwortlich und nutzt dabei die gegebenen Daten. Die Einwilligung der Nutzer beinhaltet die Zustimmung zur Verarbeitung, zur Prüfung und zur Identifizierung, falls eine Information an Nutzer wegen möglicher Risiken aus der Beratung erforderlich wird.

(4.2) Ziel:

Für die Qualitätskontrolle ist ein Personenbezug nur im Ausnahmefall (Information an Nutzer) notwendig. Dafür muss die Verbindung Daten<>Person erhalten bleiben. Zur Datenminimierung und Vertraulichkeit, aber nicht für die generelle Qualitätskontrolle.

(4.3) Eine Lösung:

Mit der Pseudonymisierung werden im Backend nur Daten ohne Personenbezug verarbeitet. Nur in seltenen Fällen, in denen eine Person über etwas zu informieren ist, gewährt die Abteilung „Pseudonym“ den Zugriff auf die personenbezogenen Daten in diesem Einzelfall.

i) Öffentlich zugängliche Daten und Werbung

In einem Urteil des Bundesverwaltungsgerichts vom 29.01.2025 mit Az. 6C.3.23¹³ geht es um die Nutzung öffentlich zugänglicher Telefonnummern zu Marketingzwecken. In diesem Fall ging es um die Speicherung von Adressdaten zu Inhabern von Zahnarztpraxen zu werblichen Zwecken (Ankauf Edelmetallreste). Kurz gesagt: Das „berechtigte Interesse des Verantwortlichen“ nach [Art.6 DSGVO](#) sieht zwar die Möglichkeit (Rechtsgrund der Verarbeitung) nach Abwägung der Risiken für die Betroffenen vor, hebt aber nicht die Regelung des [§7 Abs.2 Nr.1 des Gesetzes gegen den unlauteren Wettbewerb](#) aus. Auszug:

(2) Eine unzumutbare Belästigung ist stets anzunehmen (Nr.) 1. bei Werbung mit einem Telefonanruf gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung oder gegenüber einem sonstigen Marktteilnehmer ohne dessen zumindest mutmaßliche Einwilligung.

Von der Informationspflicht nach [Art.14 DSGVO](#), wenn die Daten nicht direkt beim Betroffenen erhoben werden mal ganz abgesehen.

j) Datenverarbeitung des Betriebsarztes

Im „Netzwerk Datenschutzexpertise“¹⁴ gibt es eine interessante rechtliche Betrachtung zur Datenverarbeitung von Betriebsärzten.¹⁵ Die Komplexität kann ich nicht besser zusammenfassen:

Die betriebsärztliche Datenverarbeitung und die damit verbundene Dokumentation von Gesundheits-

¹³ Quelle: Bundesverwaltungsgericht: „[Pressemitteilung Nr. 5/2025 vom 29.01.2025](#)“

¹⁴ Link: <https://www.netzwerk-datenschutzexpertise.de/>

¹⁵ Quelle: Netzwerk Datenschutzexpertise: „[Die Datenverarbeitung des Betriebsarztes](#)“

daten weist gegenüber sonstigen Formen ärztlicher Datenverarbeitung eine Besonderheit auf: Nicht nur das Medizinrecht und das Datenschutzrecht kommen zur Anwendung, sondern zudem das Arbeitsrecht, das Mitbestimmungsrecht und die dort bestehenden spezifischen Regelungen. Mit der Wirksamkeit der Europäischen Datenschutz-Grundverordnung kam ergänzend zu den nationalen Regelungen eine europäische Regelungsebene hinzu. (Zitat siehe LINK Einleitung zu „Die Datenverarbeitung des Betriebsarztes“)

Von mir hier nur ein paar grundlegende Dinge. Mit dem Behandlungsvertrag gilt das Arzt-Patientenverhältnis und die ärztliche Schweigepflicht. Die Betriebsärzte sind gegenüber den Arbeitgebern weisungsfrei, d. h. eine Weitergabe von Gesundheitsdaten bedingt immer eine gesetzliche Verpflichtung (z. B. Arbeitssicherheit) oder eine gesetzliche Befugnis (z. B. Einwilligung).

Für die Verarbeitung besonderer Kategorien (u. a. Gesundheitsdaten) personenbezogener Daten gelten die Vorschriften [Art.24, 25 DSGVO](#) und [§ 22 BDSG](#), die zur Datensicherheit vorgeschriebenen technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik und der Implementierungskosten im Verhältnis zum Risiko für die Betroffenen. Jetzt gibt es dazu keine konkreteren Ausführungen, aber festgehalten werden kann:

- ▶ Verantwortlich sind bei externen Betriebsärzte:innen sie selbst und bei internen der Arbeitgeber. Für die Daten gilt immer die ärztliche Schweigepflicht.
- ▶ Nicht zu vergessen, dass auch für die papierhafte Dokumentation entsprechende technische und organisatorische Maßnahmen zum Schutz vor dem Zugriff / Zugang von Dritten zu treffen sind.
- ▶ Entscheidend für mich ist, dass bei der elektronischen Verarbeitung eine Verschlüsselung der Daten vorgenommen wird (mindestens eine Zugriffsbegrenzung / -berechtigung nur für Betriebsärzte:innen und Hilfspersonal).
- ▶ Die IT-Dienstleister der Betriebsärzte:innen sind „Gehilfen“ oder „Mitwirkende“ im Sinne des [§ 203 Abs.1 StGB](#) (Verletzung von Privatgeheimnissen) und unterliegen der ärztlichen Schweigepflicht. Stellt der Arbeitgeber die IT-Dienstleistung, sind die Administratoren auf die Schweigepflicht hinzuweisen!
- ▶ Auch bei IT-Administratoren sollte der Zugriff auf ein Mindestmaß beschränkt werden.

k) Hinweis zum Datentransfer mit den USA

Es ist schon schön bequem, wenn ein angemessenes Schutzniveau nach DSGVO in dem Land der Datenverarbeitung der Organisation vorherrscht, dass durch die EU geprüft und mit einem Angemessenheitsbeschluss bestätigt ist ([Art.45 DSGVO Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses](#)). Dieser Angemessenheitsbeschluss der EU für die USA, der einen vereinfachten Datenaustausch zwischen der EU und den USA ermöglicht, steht unter Beobachtung und könnte durch rechtliche Herausforderungen und politische Entwicklungen gefährdet sein. Ausführungen dazu am Beispiel der Artikel:

- ▶ **„Trump bedroht wichtigen Daten-Deal – Wirtschaft schlägt Alarm“ (Handelsblatt 03/25)**¹⁶. Unter anderem wurden alle Mitarbeiter eines für den Datenschutz zentralen Gremiums, dem „Privacy and Civil Liberties Oversight Board (PCLOB)“, bis auf einen Mitarbeiter entlassen.
- ▶ **„Trump könnte Microsoft und Meta zwingen, Europa zu verlassen“ (INFOsperber 05/25)**¹⁷. Wie alle anderen Anbieter aus den USA auch.
- ▶ **„Microsoft kann US-Zugriff auf EU-Cloud nicht verhindern“ (Dr. Datenschutz 07/25)**¹⁸. So der Chefjustiziar von Microsoft France bei einer öffentlichen Anhörung vor dem französischen Senat des Parlaments zu den Senatsmitgliedern.

Es gibt derzeit mehrere Klagen und Beschwerden gegen die Datenübermittlung zwischen der EU und den USA, insbesondere im Zusammenhang mit dem „EU-US Data Privacy Framework (DPF)“. Diese beziehen sich hauptsächlich auf die Frage, ob das Datenschutzniveau in den USA ausreichend ist, um den Anforderungen der Europäischen Datenschutzgrundverordnung (DSGVO) zu genügen. Nur auf das Prinzip: „Hoffnung“ zu setzen, kann und ist mit recht großen Risiken ver-

¹⁶ Quelle: Handelsblatt: „[Trump bedroht wichtigen Daten-Deal – Wirtschaft schlägt Alarm.](#)“

¹⁷ Quelle: INFOsperber: „[Trump könnte Microsoft und Meta zwingen, Europa zu verlassen](#)“

¹⁸ Quelle: Intersoft consulting: „[Microsoft kann US-Zugriff auf EU-Cloud nicht verhindern!](#)“

bunden. Mit Plan B sollten mögliche Risiken gelindert (bis vermieden) werden. Ansätze:

- ▶ Basiert der aktuelle Datentransfer in die USA auf der Grundlage des „EU-US Data Privacy Frameworks“ sollte die Vereinbarung möglichst um die EU-Standardvertragsklauseln erweitert werden. Diese treten nur in Kraft, wenn der Angemessenheitsbeschluss der EU für die USA entfällt (temporäres Sicherheitsnetz).
- ▶ Es ist hilfreich, sich bereits jetzt nach alternativen Anbietern aus Europa umzuschauen. Das ist keine leichte Aufgabe und wird Zeit brauchen, den richtigen Anbieter für sich zu finden. Einige namhafte Akteure sind bereits auf dem Weg, wie der Presse zu entnehmen. Zwei Beispiele:
 - Schleswig-Holstein macht LibreOffice zur Standard-Office-Lösung in der Verwaltung und setzt auf das Betriebssystem Linux¹⁹.
 - LibreOffice ersetzt Microsoft 365 in der dänischen Regierung: eine strategische Wende²⁰.

Man muss nicht „mit der Brechstange“ an das Thema gehen, aber ein „Plan B“ kann nicht schaden.



1) Künstliche Intelligenz (KI oder AI) und der Datenschutz

Es zeichnen sich steigenden Nutzerzahlen bei allen KI-Tools ab. Jedoch bietet die Nutzung nicht nur Vorteile (wie immer), sondern auch Nachteile. Die Integration in tägliche Arbeitsabläufe bieten das Potenzial für unbefugte Weitergabe, Missbrauch und Offenlegung von internen und/oder geschützten Firmendaten und personenbezogenen Daten. Im Blog von Incogni, laut Süddeutscher Zeitung ein automatisierter Service von [Surfshark](#) mit dem Ziel, persönliche Daten aus Datenbanken von Datenbrokern zu löschen²¹, werden verschiedene KI-Modelle auf ihre Datenschutzfreundlichkeit und Fähigkeiten analysiert²². Zitat:

„Obwohl diese Tools die Produktivität steigern können, sind sich die meisten Nutzer der komplexen Datenschutzprobleme hinter den Kulissen nicht bewusst.“

Einer Analyse unterzogen wurden ChatGPT von OpenAI, Meta AI, Gemini von Google, Copilot von Microsoft, Grok von xAI, Claude von Anthropic, Pi AI von Inflection AI, das französische Modell Le Chat von Mistral AI und das chinesische KI-Modell DeepSeek.



(1) Die vorderen Plätze:

Le Chat verletzt demnach am wenigsten die Privatsphäre seiner Nutzer. Das französische KI-Modell ist im Ranking dicht gefolgt von ChatGPT auf Platz zwei.



(2) Die hinteren Plätze:

Die hinteren Plätze in Bezug auf Datenschutz belegen die große Techkonzerne Google Gemini und Microsoft Copilot mit Schlusslicht Meta AI.



(3) Beispiel: Datenschutzrisiken von Microsoft 365 Copilot

In einem Fachbeitrag hat sich „Dr. Datenschutz“ (bzw. intersoft consulting services) damit auseinandergesetzt²³. Die Kernpunkte:

- Die KI gestützte Assistenzfunktion ist gleich in die Office-Umgebung integriert, um durch Analyse die tägliche Arbeit zu erleichtern und wie ein Produktivitätsschub zu wirken.
- Neben der klassischen ChatGPT Funktion hat der Copilot zusätzlich Zugriff auf die Unternehmensdaten, mit der Möglichkeit, Inhalte über verschiedene Anwendungen hinweg zu verarbeiten.
- Dabei ist die Entscheidungsfindung und die mögliche Verarbeitung zu Microsofts eigenen Zwecken intransparent. Durch die fehlende Transparenz ist es auch schwierig, eine Rechtsgrundlage für die Verarbeitung nach DSGVO zu finden.
- Wird das Web-Plugin (Bing-API) aktiviert, wird mit den Inhalten auf das Web zugegriffen.

¹⁹ Quelle: OSB ALLIANCE: „[Schleswig-Holstein macht LibreOffice zur Standard Office-Lösung in der Verwaltung](#)“

²⁰ Quelle: hfrance.fr/de: „[LibreOffice ersetzt Microsoft 365 in der dänischen Regierung: eine strategische Wende](#)“

²¹ Quelle Süddeutsche Zeitung: „[Was ist der Datenlöschdienst Incogni?](#)“

²² Quelle Incogni | blog: „[Gen AI and LLM Data Privacy Ranking 2025..](#)“

²³ Quelle: Dr. Datenschutz: „[Datenschutzrisiken von Copilot für Microsoft 365](#)“

Wie, warum und mit welchem Schutz, bleibt intransparent.

- Copilot hat Zugriff auf alle Inhalte, auf die auch der Nutzer einen Zugriff hat (Mail, Kalender, Ordner, Dokumente u. ä.). Es fehlt also ein klar definiertes Berechtigungskonzept.

(4) **KI-Trainingsdaten mit personenbezogenen Inhalten gefunden**

T3n berichtet von sensiblen Daten im größten öffentlichen KI-Trainingsset²⁴. Obwohl Forscher erst 01 % der Daten in einem der größten Open-Source-Trainingsdatensätze für KI-Bildgeneratoren untersuchen konnten, fanden sie Millionen von Bildern aus Reisepässen, Ausweisen, Kreditkarten, Geburtsurkunden und anderen Dokumenten, die personenbezogenen Daten enthalten. Zitat:

„Laut William Agnew, Postdoktorand im Bereich KI-Ethik an der Carnegie Mellon University und Mitautor der Studie, lässt sich daraus der (alte bekannte) Schluss ziehen, dass „alles, was man online stellt, gesammelt werden kann und wahrscheinlich auch schon gesammelt wurde“. Die Forschenden fanden Tausende Fälle nachweisbar korrekter Privatdokumente.“

Das ist die andere Seite der KI-Modelle. Ich denke, die Nutzung schützt nicht vor der Verletzung von Schutzrechten Dritter (z. B. Daten- oder Urheberrechtsschutz u. ä.). Genauso könnten eigene Daten von Dritten fälschlicherweise verwendet werden.

m) **Einsatz von KI im Unternehmen**

Laut einer Ifo – Studie aus Juni 2025²⁵ setzten deutsche Firmen zunehmend auf KI. In 41 % der Unternehmen ist KI bereits im Einsatz. 19 % planen den Einsatz in den kommenden Monaten. Laut einer GOLEM-Studie²⁶ schaffen allerdings nur wenige Firmen die mit KI gesetzten Ziele (z. B. Umsatzwachstum) zu erreichen. Das liegt laut Studie weniger an der Qualität der Tools noch an den regulatorischen Beschränkungen. Es ist vielmehr die Art und Weise wie die Integration erfolgt.

Kontraproduktiv ist der Studie nach, dass mehr als die Hälfte des KI-Budgets in den Unternehmen in Sales- und Marketing-Tools gesteckt werde. Dabei ergebe sich der größte Gewinn, wenn einfache Bürotätigkeiten automatisiert würden. Damit ließen sich externe Dienstleistungen und Agenturen einsparen, interne Prozesse verschlanken und mehr Zeit für den Vertrieb gewinnen.

(1) **Fazit einer Studie:**

Unternehmen sollten eher auf extern entwickelte KI-Tools von darauf spezialisierten Anbietern setzen, als auf selbst entwickelte Lösungen. Bei Ersteren lag die Erfolgsquote immerhin bei 2/3, bei Letzteren nur bei 1/3.

(2) **Die bessere, europäische Antwort zu KI**

Und dass es Europa sogar besser kann, zeigt der FOCUS-Online in seinem Artikel „KI-Wettstreit“²⁷. Ich zitiere:

(2.1) **Wer ist Mistral**

„Sie nennen sich die französische Antwort auf OpenAI. Doch Mistral AI ist mehr als das: Es ist der Beweis, dass Europa im KI-Rennen nicht nur mitspielen, sondern die Regeln neu schreiben kann. Von null auf demnächst zehn Milliarden Dollar Bewertung innerhalb von zwei Jahren lautet ihre Bilanz. Fast 400 Mitarbeiter. Frankreichs beliebteste KI-App.“

(2.2) **Was ist Mistral**

„Während Konkurrent OpenAI seine Modelle wie ein Staatsgeheimnis hütet, macht Mistral das genaue Gegenteil: Open-Source-first nennt sich die Methode. Viele Mistral-KI-Modelle sind frei verfügbar, was eine Kampfansage an die Geheimniskrämer im Silicon Valley ist und gleichzeitig eine Strategie, um Entwickler und Kunden, die es hassen, nicht eingeweiht zu sein, auf die eigene Seite zu ziehen.“

(2.3) **Datenschutz statt Datenklau**

„Die Franzosen bauen unter der strengen EU-Regulierung eine souveräne KI-Infrastruktur auf. Ihr Versprechen: Europäische Daten bleiben in Europa. Die Strategie zahlt sich aus.“

²⁴ Quelle t3n: „[Forscher finden sensible Daten in einem der größten öffentlichen KI-Trainingssets](#)“

²⁵ Quelle Ifo Institut „[Unternehmen setzen immer stärker auf künstliche Intelligenz](#)“

²⁶ Quelle GOLEM: „[KI-Millionen verpuffen](#)“

²⁷ Quelle FOCUS-Online: „[KI-Wettstreit: Mistral vs. OpenAI: Wie drei europäische Forscher das Silicon Valley herausfordern!](#)“

Neben der interessanten Information zu Mistral sollte dies nur ein Hinweis sein, sich beim ersten Einsatz von KI an einen externen Dienstleister zu wenden, auch wenn es am Anfang etwas teurer ist, gespart wird dann am langen Ende.

n) Mein Datenschutzstatus schnell ermittelt

Das Bayrische Landesamt für Datenschutzaufsicht hat für Soloselbstständige und KMU (aus Handel, aber auch für viele andere Bereiche nutzbar) eine Checkliste zur Umsetzung datenschutzrechtlicher Anforderungen erstellt und [hier](#) veröffentlicht²⁸.

Die Checkliste ist (nicht nur) für Handels- und Dienstleistungsunternehmen und Selbstständige im B2B und teilweise im B2C Geschäft mit Endverbrauchern interessant und geeignet. Mit wenig Text und einer übersichtlichen Anzahl von Fragen (Checks) werden die wichtigen Datenschutzaspekte strukturiert im Selbsttest geprüft. Dies auch zu Themen Cloud, Messenger, Tracking, Werbung oder KI und das auf nur 13 übersichtlichen Seiten mit sehr kurzen, aber verständlichen Erläuterungen 👍. Dazu gibt es in Anlage A ein Muster zum: „*Verzeichnis der Verarbeitungstätigkeiten inkl. Compliance-Erweiterung*“ und in Anlage B eine Checkliste zu den: „*technischen und organisatorischen Maßnahmen*“.

Fazit: Sehr zu empfehlen! ★★★★★.

o) Nicht jeder darf „Datenschutzbeauftragter“

(1) Wenn, wann?

Keine Bestellpflicht, wenn weniger als 20 Personen mit der Verarbeitung beschäftigt UND keine geschäftsmäßige Datenübermittlung oder zu Markt- und Meinungsforschung UND kein hohes Risiko ([§ 38 Abs.1 BDSG](#)) besteht.

(2) Wenn, wen?

Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt ([Art.37 Abs.5 DS-GVO](#)). Seine Aufgaben umfassen (nur) Unterrichtung und Beratung, Überwachung und Einhaltung, Beratung zu Folgenabschätzungen, Zusammenarbeit und Ansprechpartner für die Aufsichtsbehörden und Anlaufstelle für Betroffene. ([Art. 39 Abs.1 DS-GVO](#)).

(3) Wenn, wen nicht!

Dazu gibt es in [Art.38 DSGVO Abs.6 und 3](#) eindeutige Aussagen, die auch gerne mal bei der Benennung von internen Datenschutzbeauftragten übersehen werden.

„(6) Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.“

„(3) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. ...“

Zur Benennung als Datenschutzbeauftragter sind trotz bester, möglicher Qualifikation auf jeden Fall wegen Interessenkonflikten ausgeschlossen:

- Leitung der Unternehmung oder der Organisation
- Leitende Angestellte, sofern sie über die Verarbeitung personenbezogener Daten entscheiden
- Verantwortliche für die IT-Sicherheit, da Konflikt zur gleichzeitigen Bewertung ausreichender technischen und organisatorischen Maßnahmen besteht.

Kann oder soll kein externer Datenschutzbeauftragter benannt werden und ist damit eine Doppelrolle unvermeidbar, sind aktive Maßnahmen zu ergreifen:

- ☒ Nachweisbare und wirksame Maßnahmen zur Vermeidung von Interessenkonflikten, einschließlich ausreichender Qualifikation
- ☒ Sorgfältige Dokumentation der Überlegungen und der Abwägung zu den Maßnahmen zur

Vermeidung der Interessenkonflikte.

Regelmäßige Überprüfung, was i. d. R. 1x pro Jahr erfolgen sollte.

In Österreich hat die Aufsicht bereits eine Geldstrafe dazu verhängt²⁹. Die Behörde betonte, dass die bloße Behauptung, es bestehe kein Interessenkonflikt, nicht ausreicht. Vielmehr müssen aktive, nach außen sichtbare Maßnahmen ergriffen werden, um potenzielle Konflikte zu verhindern.

p) Automatische Webseitenprüfung der Aufsicht

„Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat erstmals eine automatisierte Webseitenprüfung durchgeführt und dabei Verstöße bei der Einbindung von YouTube-Videos auf Webseiten des Bundes identifiziert.“ (Zitat³⁰)

Bei 500.000 geprüften Webseiten, wurden 40 Verstöße festgestellt. Auch wenn es hier zunächst um den Praxistest bei Webseiten von Behörden geht, ist eine Ausweitung auf weitere Bereiche nicht auszuschließen. Zu einer datenschutzkonformen Einbindung von Videos gilt:

- ✓ Goldstandard ist natürlich Selbsthosting auf eigenen Servern ohne Drittanbieter
- ✓ Die Zwei-Klick-Lösung, d.h Nutzer müssen zur Einwilligung der Übermittlung ihrer personenbezogenen Daten (z. B. IP-Adresse u. ä.) aktiv auf ein erklärendes Vorschaubild klicken, bevor mit einem weiteren Klick das Video auf einer Videoplattform gestartet werden kann.

Mehr Information zum Hochladen und Einbinden von eigenen und fremden Videos gibt es beim LfDI – Baden-Württemberg³¹.

q) „Viel zu klein für eine Prüfung der Datenschutzaufsicht?“

Vorsicht, ja, vom Grundsatz sind die Aufsichtsbehörden mit den großen „Datenverarbeitern“ beschäftigt, aber sie müssen auch jeder Beschwerde eines Bürgers nachgehen. Fehlt es an notwendiger Vorbereitung ist eine Prüfung mit viel Zeit, Aufwand und Ärger verbunden, abgesehen von der Höhe eines möglichen Bußgeldes. Von aktuellen Fällen kann ich ja schlecht berichten, aber bei den Tätigkeitsberichten der Aufsichtsbehörden lassen sich viele vergleichbare Fälle ablesen.

(1) Auslöser:

Anlass oder Auslöser einer Prüfung sind unzufriedene Kunden, Mitarbeiter und auch Geschäftspartner. Versehen (Fehler) gegenüber Dritten, die nicht sofort korrekt kommuniziert werden. Vermehrt gehen die Aufsichtsbehörden auch automatisiert vor, in dem die Datenschutzvorschriften z. B. auf Webseiten geprüft werden.

(2) Einfache (Bußgeld) Gründe dafür

► Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat in einer Zwischenbilanz³² mitgeteilt, in drei Fällen haben Unternehmen Kund:innen Werbung per E-Mail zugesandt, ohne dass die Empfänger:innen darin eingewilligt hatten. Gegen diese Unternehmen wurden Bußgelder im unteren fünfstelligen Bereich festgesetzt.

► Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz³³ erließ ein Bußgeld gegen eine Arztpraxis. Diese hatte einer Patientin eine Rechnung geschickt, die jedoch eigentlich für eine andere Patientin mit ähnlichem Namen hätte gehen sollen. Die Patientin, die fälschlicherweise Post erhielt, war jedoch bereits seit über zehn Jahren keine Patientin mehr in der Praxis; diese hätte ihre Daten also längst löschen müssen. Das Bußgeld fiel in den vierstelligen Bereich.

► Im Tätigkeitsbericht der Sächsischen Datenschutz- und Transparenzbeauftragten 2024³⁴ lautet es: Die Sächsische Datenschutz- und Transparenzbeauftragte erließ zwei Bußgelder gegen Privatpersonen, die in den Gebäuden, in denen sich ihre Mietwohnungen befanden,

²⁹ Quelle: 360.lexisnexis.at: „GZ: 2024-0.641.771 vom 16. Oktober 2024 (Verfahrenszahl: DSB-D550.769)“

³⁰ Quelle: BfDI: „Erste automatisierte Webseitenprüfung der BfDI deckt zahlreiche unzulässige YouTube-Einbettungen auf.“

³¹ Link: LfDI-Baden-Württemberg: „Einbindung von Videos in eigene Webseiten“

³² Quelle: HmbBfDI: „Zwischenbilanz 2025“

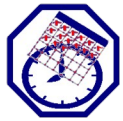
³³ Quelle: LFDI-RLP: „Best of Datenschutz 2024/25“

³⁴ Quelle: Sächsische Datenschutz- und Transparenzbeauftragte: „Tätigkeitsbericht 2024“

Überwachungskameras angebracht hatten. Diese erfassten den Hausflur bzw. den öffentlichen Verkehrsraum vor dem Haus. Die Strafen lagen zwischen 100 EUR und 1.000 EUR.



► Die Sächsische Datenschutz- und Transparenzbeauftragte erließ 12 Bußgelder gegen Privatpersonen. Diese hatten unrechtmäßig Dashcams in ihren Fahrzeugen angebracht und betrieben. Die Strafen liegen zwischen 100 EUR und 1.000 EUR.



► Die Sächsische Datenschutz- und Transparenzbeauftragte erließ zwei Bußgelder gegen Unternehmen, die nur sehr verspätet auf Informationsanfragen reagiert hatten. In beiden Fällen halfen auch Zwangsmittel nichts. Eines der Unternehmen antwortete erst nach zwei Jahren, vier Monaten und fünf Zwangsgeldern, von denen vier bezahlt wurden. Bei dem anderen brauchte es ein Jahr und vier Gelder, drei davon bezahlt.



► Die österreichische Datenschutzbehörde³⁵ verhängte ein Bußgeld gegen eine Werbeagentur. Es hatte einen Angriff auf deren Webseite gegeben, der zu einer Datenkompromittierung führte. Diesen meldete das Unternehmen nicht.

Thomas Fuchs, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: „Wenn Unternehmen auf Auskunfts- und Informationsansprüche systematisch nicht oder nur unzureichend reagieren, ist eine spürbare Sanktion geboten. Dies gilt insbesondere bei Strukturen, die für die Betroffenen undurchsichtig sind, wie Adresshandel oder komplexe Entscheidungsalgorithmen –und immer mehr auch für den Einsatz künstlicher Intelligenz. Entscheidet eine Software über Menschen, muss die verarbeitende Stelle die tragenden Gründe verständlich erklären können.“

r) Gültigkeit der Einwilligung³⁶

Die Gültigkeit einer Einwilligung gemäß der DSGVO ist von verschiedenen Faktoren abhängig.

- Eine Einwilligung muss freiwillig, spezifisch, informiert und eindeutig sein, um rechtlich gültig zu sein.
- Sie erlischt nicht automatisch durch Zeitablauf; die Rechtsprechung besagt, dass eine Einwilligung grundsätzlich nicht allein durch Zeitablauf erlischt.
- Unternehmen sollten die Freiwilligkeit und Aktualität der Einwilligung regelmäßig hinterfragen und Daten nur so lange speichern, wie sie für den ursprünglichen Zweck erforderlich sind.
- Bei medizinischen Registern gibt es keine festgelegte Gültigkeitsdauer, und die Datenschutzbehörde empfiehlt, die Einwilligung regelmäßig zu überprüfen.

Diese Aspekte sind entscheidend für die rechtliche Gültigkeit und Wirksamkeit einer Einwilligung.

Ein paar Beispiele:

(1) **Z. B. Talentpool mit Bewerberdaten**

Ob Initiativbewerbungen oder stellen-bezogene Bewerbungen, wird der Bewerber nicht direkt eingestellt, besteht für ihn die Möglichkeit mit seiner Einwilligung in den „Talentpool“ der Firma aufgenommen zu werden. Wie lange sind alte Bewerberdaten sinnvoll? Hilfreich für beide Seiten ist ca. alle 6 Monate den Bewerber auf seine Zustimmung und Aktualität der Unterlagen zu befragen.

(2) **Z. B. Website mit Mitarbeiterfotos**

Sicher wurde bei Aufnahme von Mitarbeiterfotos zur Darstellung zum Beispiel des Teams im Netz eine Einwilligung eingeholt. Es stellt sich die Frage nach der weiteren Veröffentlichung, wenn der Mitarbeiter ausscheidet und die Einwilligung nicht widerruft. Da jedoch der Zweck entfällt, sollten die Fotos in einer angemessenen Zeitspanne gelöscht werden.

(3) **Empfehlung:**

Einerseits ist zu prüfen, ob die Erwartungshaltung der betroffenen Person nach längerer Zeit

³⁵ Quelle: European Case Law Identifier: „[Urteil zum Bußgeld Datenschutzbehörde Österreich](#)“

³⁶ Quelle: Dr. Datenschutz: „[Gültigkeitsdauer der Einwilligung und Speicherbegrenzung](#)“

überhaupt noch eine tragfähige Rechtsgrundlage begründet; andererseits ist fortlaufend zu kontrollieren, ob die Daten für den Zweck, zu dem sie erhoben wurden, noch brauchbar sind.

s) Immer wieder E-Mail

(1) Anlass:

Wie unter anderem die Tagesschau mit „Exklusiv: Unsichere Ärztepost.“³⁷ berichtet, wurden im E-Mail-System der Praxen und Krankenhäuser Schwachstellen entdeckt. Damit die sensiblen Daten im Gesundheitswesen sicher verschickt werden, hat die Gematik als staatliche Stelle ein, als besonders sicher geltendes System KIM – Kommunikation im Medizinwesen spezifiziert. Ein Recherche-Team aus NDR, SZ und IT-Sicherheitsforschern haben Sicherheitsmängel aufgedeckt. Die Gematik (positiv hervorgehoben) hat umgehend Sicherheitsupdates zur Verfügung gestellt, die jetzt von den Praxen und Krankenhäusern umgehend einzuspielen sind.

(2) Datenschutzsicht:

Was sagt die Datenschutzaufsicht zur Kommunikation mittels E-Mail: Die Datenschutzkonferenz der Aufsichtsbehörden der Länder hat bereits im Juni 2021 eine Orientierungshilfe³⁸ zur Kommunikation per E-Mail herausgegeben. Im Jahresarchiv 2023 (Seite 23) befindet sich eine kurze Zusammenfassung dazu wie folgt:

Beim Versenden von E-Mails wird bei der Verschlüsselung nach Transport- und Inhaltsebene unterschieden. Jetzt wird bei der Transportverschlüsselung (TLS) jedoch nur der Weg vom Absender zu dessen Mailserver bzw. beteiligten Mailservern verschlüsselt. Auf den Mailservern liegt die Mail weiterhin im Klartext, also unverschlüsselt vor. Da der Schwerpunkt auf Zustellung und nicht auf Sicherheit liegt, kann auch das Niveau mit optionalem TLS (notfalls ohne) reduziert sein, oder es wird noch eine ältere TLS – Version eingesetzt. [Artikel 32 DS-GVO](#) schreibt ein angemessenes Schutzniveau nach dem Stand der Technik vor. Auf die Frage, ob eine TLS – Verschlüsselung ausreichend für personenbezogene Daten ist, ist jetzt vielfach zu lesen: „Kommt darauf an!“ Die Landesbeauftragte LFDI-NRW verweist auf die Orientierungshilfe der DSK, danach gilt:

- ✓ Bei Nutzung öffentlicher Dienstanbieter hat sich der Verantwortliche zu versichern, dass ausreichende Maßnahmen zur Einhaltung der DS-GVO gegeben sind (Einhaltung der Anforderungen des BSI – TR 03108-1)
- ✓ Normales Betroffenenrisiko: Mindestanforderung ist der Aufbau einer gesicherten TLS – Verbindung (STARTTLS; SMTPS).
- ✓ Hohes Betroffenenrisiko: Neben einer qualifizierten Transportverschlüsselung ist eine End-to-End Verschlüsselung notwendig, bzw. zwingend. Ein Indiz für hohes Risiko stellt z. B. der Mailverkehr von Berufsgeheimnisträgern dar.

Zwei wesentliche Punkte aus einem Beschluss der Konferenz der Aufsichtsbehörden³⁹ zur möglichen Nichtanwendung technischer und organisatorischer Maßnahmen auf ausdrücklichen Wunsch des Betroffenen sind:

1. „Die vom Verantwortlichen nach Art. 32 DS-GVO vorzuhaltenden technischen und organisatorischen Maßnahmen beruhen auf objektiven Rechtspflichten und stehen nicht zur Disposition der Beteiligten.“
2. „Unter Beachtung des Selbstbestimmungsrechts der betroffenen Person und der Rechte weiterer betroffener Personen kann es in zu dokumentierenden Einzelfällen möglich sein, dass der Verantwortliche auf ausdrücklichen und eigeninitiativen Wunsch der informierten betroffenen Person, einzelne Maßnahmen aus den technischen und organisatorischen Maßnahmen in vertretbarem Umfang nicht anwendet.“

³⁷ Quelle: tagesschau: „[EXKLUSIVE Unsichere Ärztepost, Schwachstellen im E-Mail-System aufgedeckt](#)“

³⁸ Quelle: DSK der Länder: „[Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail](#)“

³⁹ Quelle: DSK Beschluss: „[Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art.32 DSGVO auf ausdrücklichen Wunsch betroffener Personen](#)“

(3) Empfehlung:



Auf ein Angebot zur End-to-End Verschlüsselung von E-Mails ist nicht zu verzichten. Für einen Verzicht („nur“ TLS – Verschlüsselung) sollte in aufklärender Weise über die Risiken eine Einwilligung eingeholt werden. Bei sehr hohem Betroffenenenrisiko ist nicht auf eine End-to-End Verschlüsselung zu verzichten!

3. Zur Datensicherheit



a) DMA, DORA, DSA, KRITIS, CERT & NIS-2?

Um lange Bezeichnungen im Sprachgebrauch und in Texten zu vermeiden benutzen „wir“ gerne Abkürzungen. Zu viele Abkürzungen in einem ähnlichen oder gleichen Zusammenhang können aber auch (auf mich) verwirrend wirken und vor allem: „Wer muss was beachten, bzw. muss ich das beachten?“. Deshalb hier in aller Kürze, ein paar mit Bezug zum Datenschutz (DSGVO, BDSG) und der verbundenen Datensicherheit (BSI, IT-Grundschutz) aus dem letzten Jahr aufgegriffen:



(1) DMA – Digital-Markets-Act⁴⁰

Betroffen sind große, systemrelevante Plattformen, sogenannte „Gatekeeper“ oder „Torwächter“ mit folgenden Kriterien: € 7,5 Mrd. Umsatz, bzw. € 75 Mrd. Marktwert, mehr als 45 Mio. Endnutzern pro Monat und mehr als 10.000 gewerblichen Anbietern.

Es geht um europaweite, einheitliche Rahmenbedingungen für faire und offene digitale Märkte. Dabei geht es um Selbstbegünstigungsverbote, Regelungen zur Datennutzung und zur Dateninteroperabilität bis hin zu Diskriminierungsverboten und fairen Bedingungen. Verstöße können mit Sanktionen geahndet werden, darunter Geldbußen in Höhe von bis zu 20 Prozent des weltweiten (Konzern-)Jahresumsatzes. (Verordnung vom 01.11.2022, verbindlich seit 02.05.2023)



(2) DSA – Digital-Service-Act⁴¹

Betroffen sind Plattformen oder Suchmaschinen mit mehr als 45 Millionen Nutzern in der EU im Monat und im Durchschnitt der letzten 6 Monate.

Es geht um die Festlegung harmonisierter Vorschriften für ein sicheres und vertrauenswürdiges Online-Umfeld und Schutz der Grundrechte aus der [EU-Charta](#). Zum Beispiel müssen Online-Marktplätze dafür sorgen, dass Verbraucher sichere Produkte oder Dienstleistungen online erwerben können, mit verstärkten Kontrollen zum Nachweis der Zuverlässigkeit der Händlerangaben („Kenne deinen Geschäftskunden“). Es sind Anstrengungen zu unternehmen, um zu verhindern, dass illegale Inhalte auf ihren Plattformen erscheinen, auch durch Stichproben. (Verordnung vom 19.10.2022, verbindlich seit 17.02.2024)



(3) DORA – Digital-Operational-Resilience-Act⁴²

Betroffen sind alle Finanzunternehmen und alle damit verbundenen Informations- und Kommunikationstechnologien (ITK) in der EU. Also alles rund um Banken, Versicherungen, Zahlungsdienstleistern, Handelsplätzen (incl. Krypto-Dienste), Ratingagenturen u. ä.

Es geht um die Stärkung und Sicherung der Widerstandsfähigkeit des Finanzsektors in der EU. Dazu zählen die Grundsätze und Anforderungen an das IKT-Risikomanagement, der Austausch über Cyberbedrohungen und der Meldepflicht von schwerwiegenden Vorfällen, wesentlichen Bestimmungen zur Überwachung von externen Risikoanbietern, Grundlagen zum Test der digitalen Betriebsstabilität und dem Aufsichtsrahmen für kritische IKT-Drittanbieter.

(Verordnung vom 14.12.2022, verbindlich seit 17.01.2025)

PS: Für kleinere Unternehmen gilt der Grundsatz der Verhältnismäßigkeit ([Art.4 DORA](#)):

„... Vorschriften im Einklang mit dem Grundsatz der Verhältnismäßigkeit an, wobei ihrer Größe und ihrem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte Rechnung zu tragen ist.“

40 Quelle: EU: „[Gesetz über digitale Märkte](#)“

41 Quelle: Europäische Kommission: „[Gesetz über digitale Dienste: Fragen und Antworten](#)“

42 Quelle: European Insurance and Occupational Pensions Authority: „[Gesetz über die digitale operative Resilienz \(DORA\)](#)“

Dokument von <https://volkerschroer.de>

(4) NIS-2 (Network-and-Information-Security)⁴³

Betroffen sind Organisationen mit mehr als 50 Angestellten, mindestens € 10 Mio. Umsatz oder Bilanzsumme und der Erbringung von kritischen Dienstleistungen für die Allgemeinheit. Maßgeblich kritische Sektoren sind Energie, Transport, Bank- & Finanzwesen, Gesundheit, Trinkwasser, digitale Infrastruktur, Abwasser, öffentl. Verwaltung, Information-, Kommunikationstechnik und Weltraum. Andere kritische Sektoren sind Abfall, Lebensmittel, Chemikalien, Industrieproduktion, Forschung, digitale Dienste, Post und Kurierdienst. Organisationen müssen sich selbstständig einordnen und beim BSI registrieren.

Es geht um proaktive Sicherung der Unternehmensnetzwerke und der digitalen Infrastruktur durch Einführung eines NIS2-konformen Risikomanagements mit Bewertung und Bewältigung der Risiken. Es sind effektive Sicherheitsprogramme mit klaren Richtlinien und Verfahren für den Umgang mit Sicherheitsvorfällen zu implementieren.

(5) KRITIS – Kritische Infrastruktur (CER)⁴⁴

Ausgangsbasis ist die EU-RCE Directive bzw. die CER-Richtlinie (Critical Entities Resilience Directive (EU 2022/2557) die in Deutschland mit dem KRITIS-Dachgesetz umgesetzt wird (werden soll, da noch nicht verkündet).

Betroffen sind mit der BSI-KRITIS-Verordnung alle Unternehmen, die eine wichtige Bedeutung für die Aufrechterhaltung gesellschaftlicher Funktionen haben. Richtgröße sind 500.000 Betroffene und mehr im Falle einer Betriebsstörung in den Bereichen Energie, Wasser, Ernährung, IT, Telekommunikation, Finanzen, Versicherungen, Transport, Verkehr und Gesundheit sowie Staat, Verwaltung, Medien und Kultur.

Es geht um die Stärkung der Widerstandsfähigkeit und physische Sicherheit (Resilienz) kritischer Infrastrukturen u. a. mit Meldepflichten, einem ganzheitlichen Managementprozess (BCM), Personal und Krisenmanagement (All-Gefahren-Ansatz, d. h. jedes denkbare Risiko, von Naturkatastrophen bis Sabotage, Terror und menschliches Versagen). Zu den Pflichten gehört u. a. die Einrichtung einer Kontaktstelle, die Meldung erheblicher Beeinträchtigungen (IT-Störungen), eine IT-Sicherheit auf dem Stand der Technik und alle zwei Jahre ein Nachweis gegenüber dem BSI. Hinweis: Weitere Informationen und erste Unterstützungsangebote für die Wirtschaft bietet das BSI unter „Umsetzung der NIS-2-Richtlinie für die regulierte Wirtschaft“⁴⁵ an.

b) Manipulierte Rechnung per E-Mail

(1) Der Fall

... vor der 2. Zivilkammer des LG Rostock⁴⁶:

Der Handwerksbetrieb hatte um 14:14 eine Rechnung per unverschlüsselter E-Mail (Verfahren so vereinbart) verschickt, die erst um 14:35 beim Kunden mit geänderter Bankverbindung eingegangen war. Ein „klassischer“ Fall von „Man-in-the-Middle-Angriff“, bei dem die Mail aus dem kompromittierten System des Handwerkers abgefangen und verändert weitergeleitet wurde. Der Kunde hat auf die falsche Bankverbindung gezahlt, und der Handwerker besteht auf die Begleichung der Rechnung.

(2) Das Urteil

Der Kunde wird zur erneuten Zahlung des Rechnungsbetrages auf die korrekte Bankverbindung verurteilt bei Anspruch auf Schadenersatz wegen ungerechtfertigter Bereicherung gegen den Empfänger der ursprünglichen Zahlung. In der Begründung geht das Gericht auf ein mögliches Verschulden des Kunden ein. Zum einen hatte man sich wissentlich auf die ungeschützte E-Mail-Kommunikation geeinigt. Zudem wies die E-Mail eine fehlerhafte HTML-Formatierung auf, und der Kunde kannte die korrekte Bankverbindung des Handwerkers aus der gemeinsamen Geschäftsverbindung, d. h. es sprechen gleich 3 Gründe hier für eine erhöhte Aufmerksamkeit.

c) HP-Universal-Drucker-Treiber mit kritischer Sicherheitslücke (UPDATE !!!)

⁴³ Quelle: Secjur.com Grafik: „KRITIS vs. NIS2-Übersicht“

⁴⁴ Quelle: BSI: „Pflichten für KRITIS-Betreiber“; BfM: zu KRITIS-Dachgesetz; Open KRITIS: „KRITIS – auf den zweiten Blick“

⁴⁵ Link: BSI: „Umsetzung der NIS-2-Richtlinie für die regulierte Wirtschaft“

⁴⁶ Quelle: landesrecht-mv.de: „LG Rostock 2. Zivilkammer Aktenzeichen 2 O 450/24 vom 20.11.2024“

Heise Online⁴⁷ berichtet von einer klaffenden und kritischer Sicherheitslücke im Universal Druckertreiber, die Codeschmuggel ermögliche. Ein Update zur Behebung steht bereit und sollte umgehend installiert werden.

d) Sicherheitslücken – Risiko für die Guten

In einem Fachbeitrag beschreibt Dr. Datenschutz⁴⁸ das Problem mit der Meldung von IT-Sicherheitslücken durch die Guten, d. h. ohne diese auszunutzen. Der ganze Artikel ist in der Fußleiste verlinkt. Hier kurze Ausschnitte von mir:

- Ethische Hacker verwenden „Responsible Disclosure“, d. h. ob zufällig oder gezielt gefundene Schwachstellen werden zunächst der verantwortlichen Stelle gemeldet. Nachdem die Schwachstelle geschlossen ist, wird diese mit zeitlicher Verzögerung veröffentlicht. Damit kann diese Schwachstelle nicht mehr ausgenutzt werden und alle wissen über ein erforderliches Update.
- Statt als Verantwortlicher dankbar über die Information und der Möglichkeit der Behebung zu sein, meine manche einen Strafantrag nach [§ 202a StGB](#) (Ausspähen von Daten) zu stellen. Die bekannteste Blamage ist die der CDU. Sie verklagt eine Sicherheitsforscherin wegen Meldung einer Sicherheitslücke in einer App.⁴⁹
- Schlimmste Konsequenz, die Schwachstellen werden aus diesem Grund nicht mehr gemeldet und die „Bösen Hacker“ nutzen diese für ihren Betrug.

e) BSI empfiehlt den Wechsel von Windows 10⁵⁰

Nora Kluger, Expertin für digitalen Verbraucherschutz beim BSI:

„Sicherheitsupdates sind für die IT-Sicherheit essenziell, weil dadurch Sicherheitslücken geschlossen werden, die sonst von Angreifenden ausgenutzt werden könnten. Die weitere Nutzung von Windows 10 nach Ende des Supportzeitraums birgt daher gravierende Sicherheitsrisiken. Nutzerinnen und Nutzer sollten deshalb in den kommenden sechs Monaten zu einem Betriebssystem wechseln, für das weiterhin vollumfänglich Sicherheitsupdates bereitgestellt werden. Neben dem Upgrade auf Windows 11 ist auch der Wechsel auf ein anderes Betriebssystem (z. B.. macOS oder Linux) eine Option.“

f) BSI, KI und Captchas⁵¹

Captchas werden allgegenwärtig eingesetzt, um zwischen automatisierten Bots und echten menschlichen Nutzern durch verschiedene Aufgaben wie verzerrte Text- oder Bilderkennungsaufgaben zu unterscheiden und so böartige Aktivitäten wie Spamming, Brute-Force-Angriffe und Data Scraping zu verhindern, indem sie menschenähnliche Antworten verlangen. Aktuell warnt das Bundesamt für Sicherheit in der Informationstechnik vor einer perfiden neuen Masche: Betrüger nutzen gefälschte Captchas, um mittels einer Tastenkombination ahnungslose Nutzer zu schädigen. Die Methode klingt zunächst vertraut: Auf einer Webseite soll der Nutzer ein Rätsel lösen, um zu bestätigen, dass er kein Roboter ist – ein sogenanntes Captcha. Doch in manchen Fällen folgt darauf ein zweites Fenster, das zur Eingabe bestimmter Tastenkombinationen auffordert. Wer dieser Anweisung folgt, installiert im schlimmsten Fall unbewusst Schadsoftware auf seinem Rechner.

g) Identitätsdiebstahl

„Mit meinen Daten kann doch keiner etwas anfangen!“, Antwort: „Äh ... DOCH!“

In einem „Update Wirtschaft vom 22.05.2025“⁵² der Tagesschau werden die Möglichkeit der Kriminellen sehr klar geschildert. Zum einen eröffnen Betrüger täuschend echte Fake-Accounts von Prominenten (hier von Prof. Marcel Fratzscher vom DIW, geschildert in Minuten 0 - 10 und Anja Kohl von der ARD, geschildert in Minuten 10 - 18) um z. B. Dritte mit Anlagetipps zu verführen und zu betrügen.

47 Quelle: heise online: „[Alert: HP: Kritische Lücken in Universal-Druckertreiber ermöglichen Codeschmuggel](#)“

48 Quelle: Dr. Datenschutz (intersoft consulting services): „[Meldung von Sicherheitslücken – Risiko für die „Guten“](#)“

49 Quelle: inside digital: „[Hacker-Skandal: CDU verklagt Sicherheitsforscherin, die gravierende Lücke entdeckt hat](#)“

50 Quelle: BSI: „[BSI empfiehlt Upgrade oder Wechsel des Betriebssystems nach Supportende von Windows 10](#)“

51 Quelle: BSI: „[Einfluss von KI auf die Cyberbedrohungslandschaft](#)“

52 Quelle: Tagesschau: „<https://www.tagesschau.de/multimedia/sendung/tagesschau24/boerselive/video-1469140.html>“

Mit Daten zu Identitäten von jedermann lassen sich Bestellungen aufgeben, Kredite aufnehmen und/oder deren Bekannte, Freunde, Kollegen und Mitarbeiter zu schadhaften Handlungen bewegen, wie Felix Kühlenkamp vom Bitkom e. V. ab der 18. Minute schildert. Die Anzahl der Betroffenen ist nicht gerade klein: 61 % der Privatpersonen sind schon Betrügern mehr oder weniger stark „aufgefressen“. 81 % der Firmen wurden angegriffen. Es lohnt, sich mal „rein zu schauen!“.

h) Kündigung wegen Datenschutzverletzung

Es passiert leider immer wieder, und in manchen Fällen führt es zu harten Konsequenzen. Die Datenschutzverletzung durch einen Mitarbeiter (durch den Arbeitgeber geht auch, das aber an anderer Stelle). Aus dem Urteil des OLG München⁵³. Kurz gefasst:

Der angestellte Vorstand hatte regelmäßig Mails von seinem Firmenaccount auf seinen Privataccount umgeleitet. Obwohl laut Vertrag:

„Der Vorstand verpflichtet sich alle betrieblichen Angelegenheiten und Geschäfts- und Betriebsgeheimnisse, die ihm während und im Rahmen seiner Tätigkeit (...) bekannt werden, vertraulich zu behandeln, unabhängig davon, ob sie als vertraulich gekennzeichnet oder offensichtlich als vertraulich erkennbar sind.“

Bei den Mails handelte es sich um Themen wie Bankanfrage wegen Geldwäsche, Provisionszahlungen, Mitarbeiter, Gehälter, Unternehmensplanung. Damit hat der Kläger (gegen die Kündigung) seine Legalitätspflichten ([§ 93 Abs.1 AktG](#)) gegenüber der Beklagten (Unternehmen) verletzt und personenbezogene Daten ohne Rechtsgrundlage verarbeitet.

Fazit: Es ist keine gute Idee, ob Vorstand, Führungskräfte, Mitarbeiter, Selbstständige u. v. a. ohne klärende Absprachen Daten und Mails außerhalb einer Organisation be- bzw. verarbeiten zu wollen.

i) E-Mails, ohne geht es nicht, aber ...!

Es ist kein Geheimnis, E-Mails gehören zum beruflichen und privaten Alltag und sind da auch nicht wegzudenken. Genau deswegen sind E-Mails ein beliebtes Ziel für Betrüger und Hacker. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat neue Empfehlungen veröffentlicht⁵⁴. Ein Blick, der sich lohnt, um sich vor Datenklau, Betrug und Imageschäden zu schützen. Die Seite des BSI bietet einen umfassenden Überblick über Risiken im E-Mail-Verkehr und entsprechende Schutzmaßnahmen für Organisationen. Hier sind die wichtigsten Punkte:

(1) Bedrohungsszenarien

- **Schadsoftware-Infektionen:** E-Mails mit gefährlichen Anhängen oder Links sind häufige Einfallstore für Malware.
- **Datenabfluss & Manipulation:** Unverschlüsselte E-Mails können abgefangen, mitgelesen oder verändert werden.

(2) Schutzmaßnahmen

- **Verschlüsselung:** Zum Schutz von Vertraulichkeit und Integrität.
- **Digitale Signaturen:** Zur Sicherstellung der Authentizität von Absendern.
- **Spam-Abwehr:** Reduziert unerwünschte E-Mails und entlastet die Infrastruktur.

(3) Empfehlungen für Organisationen

- **IT-Grundschutz-Kompendium:** Enthält Bausteine und Standards zur Absicherung von E-Mail-Clients und -Servern (z. B. Microsoft Outlook, Exchange).
- **ISI-Reihe (Internet-Sicherheit):** Bietet technische und nicht-technische Leitfäden zur sicheren Nutzung und zum sicheren Betrieb von E-Mail-Systemen.

Unter den technischen Leitfäden befindet sich auch eine nicht-technische Kurzfassung für (IT-) Manager (Links): [Sichere Nutzung von E-Mail \(Isi-L\)](#), [sicherer Betrieb von E-Mail-Servern \(Isi-L\)](#).

j) BSI zu KI Systemen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) leistet Grundlagenforschung und entwickelt bedarfsorientierte wie praxisnahe Anforderungen, Prüfkriterien und Prüf-

⁵³ Quelle: OLG München. „[Endurteil v. 31.07.2024 – 7 U 351/23 e](#)“

⁵⁴ Quelle: BSI: „[E-Mail-Sicherheit](#)“

methodologien, um den Einsatz von KI zum Wohle der Allgemeinheit sicher zu gestalten. Ausführliche Informationen finden Sie auf der Webseite des BSI, die in der Fußleiste verlinkt ist⁵⁵.

Enthalten ist auch ein Kriterienkatalog für vertrauenswürdige KI-Systeme im Finanzsektor, der auch zur Orientierung in anderen Sektoren dienen kann und sich an der KI – Verordnung der EU orientiert. Weiter interessant sind auch die Qualitätskriterien für Trainingsdaten im KI – Lebenszyklus.

Ich muss allerdings gestehen, diese Dokumente nicht alle selbst gelesen zu haben, sondern mich auf die Empfehlung eines IT-Spezialisten dabei verlasse.

k) Verschnaufpause Windows 10



Mit dem Wechsel auf Windows 11 haben noch nicht alle abgeschlossen. Die einen scheuen den Aufwand, den anderen fehlt möglicherweise die vorgegebene Hardware. Ursprünglich sollte Mitte Oktober mit Sicherheitsupdates für Windows 10 Schluss sein. Danach wären nur noch kostenpflichtige Updates zu erhalten. Jetzt hat Microsoft den Supportzeitraum um ein Jahr verlängert.

Fazit: Das Problem ist also nur aufgeschoben und nicht aufgehoben!⁵⁶

l) Sicherheitshinweis für Microsoft Teams



Microsoft hat einen Sicherheitshinweis für alle Teams-Nutzer veröffentlicht⁵⁷. Darin erläutert Microsoft, wie Cyberkriminelle Teams für Social-Engineering-Angriffe nutzen, um sich Zugang zu Firmenrechnern zu verschaffen, erläutert die Angriffskette und gibt Sicherheitsempfehlungen. Und diese Warnungen und Hinweise kommen nicht zu früh, denn schon wenige Tage später, informiert Microsoft darüber, eine aggressive Angriffskampagne unterbrochen zu haben, bei der Cyberkriminelle Teams missbrauchten.

m) Bremsen Datenschutzvorschriften die KI aus, oder helfen sie sogar?



Interessante Online - Analyse dazu in CLOUDCOMPUTING INSIDER⁵⁸. Fazit :

Zitat: „Es zeigt sich also, dass die Forderungen aus dem Datenschutz den Vorgaben, die ein Unternehmen generell an den Einsatz von KI stellen sollte, nicht widersprechen, sondern vielmehr diesen entsprechen. Wer KI legal, nachvollziehbar, zielgerichtet, korrekt, mit möglichst wenig Kosten und sicher einsetzen will, fährt gut damit, den Datenschutz nach DSGVO einzuhalten, nicht nur um den gefürchteten Sanktionen zu entgehen, sondern weil die Forderungen aus dem Datenschutz generell Sinn machen und für einen höheren Erfolg bei KI-Projekten sorgen können.

Nicht der Datenschutz behindert also den KI-Einsatz, sondern eine Unsicherheit darüber, was der Datenschutz fordert und wie es sich umsetzen lässt.“

n) Handy – Richtlinie der NSA



Die NSA⁵⁹ hat bereits in 2021 eine Richtlinie zum Umgang mit Smartphones erlassen. Ein regelmäßiger Neustart löscht mögliche Schadsoftware im Zwischenspeicher, sodass der Hacker gezwungen wird, diese neu zu installieren und bei zu viel Aufwand das Interesse verliert. Außerdem werden wenig benutzte Apps, die oft permanent im Hintergrund laufen, beendet.

o) Erfasst MS-Teams die Büroanwesenheit?



Im Block von Microsoft⁶⁰ ist folgendes für den Rollout-Start: „März 2026“ angekündigt:

Enhance in-office collaboration with Microsoft Teams' new @nearby mention type. Easily notify teammates who are physically present in the office, streamlining communication and fostering real-time connections. Perfect for quick discussions or impromptu meetings, @nearby keeps your team aligned and efficient.

⁵⁵ Quelle BSI: „[Künstliche Intelligenz](#)“

⁵⁶ Quelle: tagesschau. „[Microsoft, doch weiter kostenlose Update für Windows 10](#)“

⁵⁷ Quelle: Microsoft: „[Disrupting threats targeting Microsoft Teams](#)“

⁵⁸ Quelle: CLOUDCOMPUTING INSIDER: „[Warum mehr Datenschutz in der Cloud bei KI-Projekten hilft](#)“

⁵⁹ Quelle: NSA: „[Mobil Device Best Practices Guidelines als PDF von Netzwelt bereitgestellt.](#)“ und [Netzwelt](#)

⁶⁰ Quelle: „[Microsoft 365 Roadmap for Teams](#)“

Frei übersetzt:

Verbessern Sie die Zusammenarbeit im Büro mit dem neuen @nearby-Erwähnungstyp von Microsoft Teams. Benachrichtigen Sie einfach Teamkollegen, die physisch im Büro (Anm.: Homeoffice) anwesend sind, und rationalisieren Sie die Kommunikation und fördern Sie Echtzeitverbindungen. Perfekt für schnelle Diskussionen oder spontane Meetings, @nearby hält Ihr Team ausgerichtet und effizient.

Heise.de⁶¹ bewertet es wie folgt:

„Microsoft Teams erschwert die Anwesenheitsfiktion im Homeoffice: Mit einem Update wird die Plattform den Standort eines Mitarbeiters übers Büro-WLAN verfolgen.“

Wie immer es auch funktioniert, Microsoft hat sich dazu nicht genauer ausgedrückt. Dafür hat die tagesschau⁶² in einem Artikel über die Sicherheitslücke im Alltag unter der Überschrift: „Über WLAN-Signale Menschen erkennen“, berichtet. Über WLAN-Signale lassen sich Menschen erkennen und identifizieren. Das haben Forschende des Karlsruher Instituts für Technologie herausgefunden. Die Forschenden am KIT betonen, dass dieses technisch faszinierende Verfahren nicht zur Überwachung gedacht sei. Vielmehr wolle man auf Sicherheitslücken hinweisen. Die relevanten Rückmeldesignale könnten nämlich auch verschlüsselt werden.

p) Sichere -E-Mail Verschlüsselung und ein Problem davor

Die Fragen sind, wie geht das jetzt, und wo ist das Problem?

Die meisten Systeme basieren auf Prozessabläufen von GNU Privacy Guard (englisch für „GNU-Privatsphärenschutz“), abgekürzt GnuPG oder GPG. GPG ist ein freies Kryptosystem. Es dient zum Ver- und Entschlüsseln von Daten sowie zum Erzeugen und Prüfen elektronischer Signaturen. Für die Anwendung und Integration in ein Mailprogramm gibt es verschiedene Software, einschließlich Open-Source-Software (z. B. GPG)

(1) Funktionsweise:

Zur Verwendung wird ein Schlüsselpaar generiert aus:

- ✓ einem privaten, persönlichen, geheimen, mit Passwort geschütztem Schlüssel. Mit diesem Schlüssel können Daten entschlüsselt und signiert werden.
- ✓ und aus einem öffentlichen Schlüssel. Mit diesem Schlüssel können Daten NUR verschlüsselt und Signaturen überprüft werden. Damit bestehen keine Möglichkeiten Daten zu verschlüsseln, oder zu signieren. Deshalb besteht auch kein Sicherheitsrisiko. Dieser Schlüssel kann öffentlich mit allen geteilt werden, z. B. einem Schlüsselservers im Internet.

(2) Einfaches Beispiel:

Von meinem Kommunikationspartner besorge ich mir seinen öffentlichen Schlüssel. Mit diesem Schlüssel wird die Mail an ihn verschlüsselt. Gleichzeitig wird mit meinem geheimen Schlüssel ein Signaturwert errechnet und als Signatur beigefügt.

Mein Kommunikationspartner kann mit seinem persönlichen, geheimen Schlüssel die erhaltene Mail wieder entschlüsseln und über meine öffentlichen Schlüssel den Wert der Signatur verifizieren.

(3) Und das Problem ist?

Wie kann sichergestellt werden, dass der Schlüssel von der richtigen Person vorliegt?

Da „jeder“ ein solches Schlüsselpaar für sich generieren kann, muss auf einem anderen Weg (ähnlich der 2-Faktor-Authentifizierung) der Schlüsselerhalt von der richtigen Person verifiziert werden. Möglichkeiten der Verifizierung:

- ✓ Mit einem parallelen Telefonat wird der sichere Austausch bestätigt.
- ✓ Austausch öffentlicher Schlüssel über verifizierte Internetseite
- ✓ Bildung eines „Web of Trust“⁶³, d. h. die Verifizierung erfolgt über mehrere Personen aus einem Netz des Vertrauens.

⁶¹ Quelle: heise online: „[Microsoft Teams kann ab Dezember Büroanwesenheit erfassen](#)“

⁶² Quelle: tagesschau: „[Über WLAN-Signale Menschen erkennen](#).“

⁶³ Quelle: Wikipedia: „[Web of Trust](#)“

In der Schlüsselverwaltung (hier PGPFrontend) besteht für jeden Schlüssel die Möglichkeit der Vertraulichkeitseinstufung in 5 Kategorien: „undefiniert, niemals, geringfügig, voll und ultimativ“.

(4) Hinweis:

Ich kann es schon lange, aber kaum jemand nutzt es, selbst Anfragen an den Datenschutzbeauftragten werden nicht signiert oder verschlüsselt.

4. Zu angrenzenden Themen

a) Hält der EU US-Angemessenheitsbeschluss?

Wie Datenschutzticker.de⁶⁴ berichtet, ist durch einen Trump-Beschluss das Kontrollgremium „Privacy and Civil Liberties Oversight Board“ handlungsunfähig und damit der US-Datentransfer mit dem EU-Angemessenheitsbeschluss gefährdet. Damit könnte das ganze „Drama“ von vorne beginnen.

b) Die „Dracula Suite“⁶⁵

Es ist jetzt keine Büro-Office-Suite, sondern eine Plattform für Kriminelle bereits in der Version 3.0, warnt Netcraft. Die Dracula-Suite stellt eine signifikante Veränderung der kriminellen Fähigkeiten dar und reduziert die Eintrittsbarriere für geringqualifizierte Kriminelle, um jede Unternehmensmarke zu klonen und mit komplexen, anpassbaren Phishing-Kampagnen anzusprechen. „Netcraft“ hat in den letzten zehn Monaten über 90.000 neue Dracula-Domains entdeckt und blockiert sowie zahlreiche betrügerische Websites für Kunden entfernt. Erhöhte Vorsicht ist nicht erst seit heute geboten.

c) GoBD Änderung Fristen

Nach dem vierten Bürokratienteilungsgesetz reduzieren sich die steuerrechtlichen Aufbewahrungsfristen von 10 auf 8 Jahre. Dabei sollte nicht vergessen werden, dass sich damit auch die Löschfristen um 2 Jahre verkürzen und anzupassen sind.

d) Supportende Windows 10⁶⁶

Nicht zu vergessen, der Support für Windows 10 endet nach 10 Jahren am 14. Oktober 2025, was bereits offiziell am 13.06.2021 angekündigt wurde. Damit läuft man Gefahr, potenzielles Opfer für Kriminelle zu werden, da keine Sicherheitsupdate mehr zur Verfügung gestellt werden.

(1) Alternative: Umstieg auf Windows 11

(2) Windows 10 mit kostenpflichtigem ESU-Service⁶⁷ nutzen. Wichtige und kritische Sicherheitsupdates werden jeden Monat veröffentlicht. Der Preis verdoppelt sich jedes Jahr, und auch dieser Service endet im Oktober 2028.

(3) Updates über Micropatches von OPatch⁶⁸, einem slowenischen Unternehmen namens ACROS Security. Dabei werden keine klassischen Updates für das Dateisystem, sondern die Updates werden durch das System im Arbeitsspeicher zur Verfügung gestellt. Ein Abonnement ist erforderlich.

e) Keine Werbung!⁶⁹

Neue gesetzliche Anforderungen und steigende Cyberbedrohung erfordern resiliente digitale Infrastrukturen, da ist mir in den Nachrichten aufgefallen (keine Werbung). Der Berliner Cloud- und Managed-Kubernetes-Spezialist SysEleven hat nun das ISO 27001-Zertifikat auf Basis des IT-Grundschutzes vom BSI erhalten. Damit ist das Unternehmen eine von nur zwei souveränen Cloud-Plattformen in Deutschland, die IT-Grundschutz, C5-Testierung und ISO 27001-Zertifizierung kombinieren. Als Tochter des Cybersecurity-Unternehmens Secunet Security Networks

64 Quelle: datenschutzticker.de: „[EU-US-Datenschutzrahmen durch Trump bald Geschichte?](#)“

65 Quelle: chip.de/news/cyber-security: „[Experten schlagen Alarm: Gefährliches Tool macht Betrug einfacher denn je](#)“

66 Quelle: SECURITY-INSIDER: „[Alles was Sie über das Ende von Windows 10 wissen müssen](#)“

67 Link: Microsoft: „[Esu-Programm \(Extended Security Updates\) für Windows 10](#)“

68 Link: Opatch Blog: „[Long Live Windows 10... With Opatch](#)“

69 Quelle: BSI: „[BSI erteilt ISO 27001-Zertifikat ... an Prowise](#)“, „[SysEleven GmbH erhält ISO 27001-Zertifikat](#)“

unterstreicht Sysleven damit seinen Anspruch an hohe Sicherheits- und Compliance-Standards. Das zweite Unternehmen ist die Prowise GmbH, Köln.

f) Abschaltung US-basierender Digitaldienste durch US-Regierung?

Alle US-Anbieter digitaler Dienste betonen aktuell und immer wieder, Vorkehrungen getroffen zu haben, damit die Auswirkungen einer Anweisung der US-Regierung zur Abschaltung ihrer Dienste nicht ihre europäischen Kunden treffen kann. Und es geht leider doch, wie die Associated Press News unter dem 15. Mai 2025 berichtet⁷⁰ (Ausschnitt / Zitat):

„Microsoft zum Beispiel sagte Khans E-Mail-Adresse ab und zwang den Staatsanwalt, zu Proton Mail, einem Schweizer E-Mail-Anbieter, zu wechseln, sagten ICC-Mitarbeiter. Seine Bankkonten in seinem Heimatland Großbritannien wurden blockiert.“

Einen Plan B kann da nicht schaden, da jeder auch unter Kollateralschaden fallen kann.

g) Praktische KI (AI)

Es findet sich eine erste Veröffentlichung einer LegoGPT mit Code und Demo⁷¹, die Bauanleitungen anhand von Vorgaben und dem Bestand an Steinen entwerfen soll. Wo früher Rechenschieber und heute Computer eingesetzt werden, ist dies ein schönes Beispiel wofür im Unternehmensumfeld ein „Generative Pretrained Transformer = GPT“ eingesetzt werden kann.

h) KI aus Europa?

Beim Überfliegen der Nachrichtenübersicht hat diese Überschrift „*Das sind die KI-Stars aus Europa: Diese KI-Modelle aus Europa sind Weltspitze*“⁷² dann doch mein Interesse geweckt. Der Artikel ist in der Fußleiste verlinkt. Auszüge:

„Vom Gesundheitswesen über das Finanzwesen bis hin zur Umweltüberwachung – europäische KI-Modelle sind in zahlreichen Branchen führend.“

Wer also künstliche Intelligenz für sein Unternehmen / Unternehmung einsetzen möchte, kann auch in Europa faire, datenschutzkonforme Spitzenleistung bei der Entwicklung erwarten. Beispiele sind DeepMind aus Großbritannien mit AlphaGo, die App schlug den weltbesten Go-Spieler, oder AlephAlpha aus Heidelberg mit natürlichen Sprachverarbeitungsmodellen, oder ABBYYY aus München mit einer optischen Zeichenerkennung für geschriebene oder gedruckte Texte im Finanzwesen und und und. Ich glaube „DIE“ brauchen nur die richtige Aufgabenstellung, um eine große Hilfe für Unternehmen zu entwickeln.

i) Mal einen Blick auf Geldbußen für DSGVO-Verstöße in Deutschland 2025

(1) € 45 Mio. „unzureichend“

Unzureichende Überprüfung und Überwachung von Unterauftragnehmern ([Details](#))

(2) € 120.000 „verspätet“

Drastisch verspätete Reaktion auf Auskunftersuchen ([Details](#))

(3) € 30.000 „unerlaubt“

Unerlaubte Videoüberwachung ([Details](#))

j) Paypal aber sicher⁷³

In dem verlinkten Beitrag wird auf die aktuellen Probleme (Datenleck, Lastschriftenblockade) von Paypal eingegangen. Zu den Schutzmaßnahmen gehört – genau – 2-Faktor-Authentisierung beim Login, dann „klappt es auch problemlos mit dem bezahlen.“ 😊

k) Dringliche Sicherheitswarnung von Samsung wegen WhatsApp

Dieser Artikel unter techbook.de⁷⁴ fällt für unter die Kategorie: „Das kann doch nicht sein, oder?“

Auf der eigenen Website teilt Samsung mit, dass eine Schwachstelle von Cyberkriminellen bereits aktiv im Zusammenhang mit WhatsApp genutzt wird. Dieses Problem liegt vornehmlich

⁷⁰ Quelle. AP. „Trump's sanctions on ICC prosecutor have halted tribunal's work“

⁷¹ Quelle: github: „Generating Physically Stable and Buildable Brick Structures from Text.“

⁷² Quelle. Techzeitgeist.de: „Das sind die KI-Stars aus Europa: Diese KI-Modelle aus Europa sind Weltspitze“

⁷³ Quelle tagesschau.de: „Wie sicher ist PayPal als Zahlungsmethode?“

⁷⁴ Quelle: TECHBOOK: „Kritische Probleme - Dringliche Sicherheitswarnung von Samsung wegen WhatsApp.“

beim beliebten Messenger vor, weshalb Samsung wegen WhatsApp eine entsprechende Warnung veröffentlicht hat. Die Schwachstelle gilt für alle Geräte mit Android 13 oder höher als kritisch.

Samsung und WhatsApp haben bereits Updates bereitgestellt ... A B E R:

Anders als bei anderen Unternehmen wie Apple oder Google gibt es bei Samsung bestimmte Update-Reihenfolgen, je nach Modell, Region und sogar Mobilfunkanbieter. Eigentümer eines Galaxy-Gerätes sollten nach einem neuen Update Ausschau halten. Wie lange es konkret dauern wird, bis es auch bei ihnen bereitsteht, ist aber nicht bekannt.

l) **Nützliche Informationen – verständlich!**

Vom Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt es hilfreiche Informationen als Broschüren, die nicht nur für Verbraucher interessant sind⁷⁵. Unter [Wegweiser im digitalen Alltag](#), befindet sich eine Liste mit vielen Themen, unter anderem zu:

✓ **Checklisten für den Ernstfall (Was ist zu tun!):**

Gehackter Account, Erpressung mit Nacktbildern, Phishing, Betrug beim Onlinebanking, Cybermobbing unter Kindern und Jugendlichen und Infektion mit Schadprogrammen.

✓ **Wegweiser kompakt (Wie schützen bzw. vorbeugen!):**

Tipps für mehr E-Mail-Sicherheit, künstliche Intelligenz sicher nutzen, 8 Tipps für den digitalen Familienalltag, Schritt für Schritt zu Jugendschutzeinstellungen bei Apps, Spielen & Co., 8 Tipps für den sicheren Umgang mit Smart Speakern, Schritt für Schritt: Zwei-Faktor-Authentisierung für Gamingaccounts und Konsolen, Schritt für Schritt zum Gäste-WLAN, Schritt für Schritt zur Datensicherung, Schritt für Schritt automatische Updates einrichten, 8 Tipps für ein sicheres Heimnetzwerk.

Für die meisten Leser natürlich alles eine Selbstverständlichkeit, aber es lohnt sich das eine oder andere Thema nochmal kurz durchzulesen. Die Checklisten sind bestimmt gut zur Vermeidung von Unruhe im Ernstfall. Auch eine gute Empfehlung für nicht so versierte Dritte, wenn man selbst knapp in der Zeit ist sich zu kümmern.

m) **„Ich bin doch uninteressant für Hacker, oder?“**

Jede Identität, je besser auskundschaftet, hat einen großen Wert für Kriminelle. Damit lassen sich zum Beispiel im Ausland Konten eröffnen und Geld waschen, ohne Informationen darüber selbst zu erhalten, von Social-Engineering nicht zu sprechen. Security Insider berichtet von einem alarmierenden Anstieg gestohlener Zugangsdaten. Cyberkriminelle greifen nach digitalen Identitäten⁷⁶. Nach einer Studie von Cyberint ist ein Anstieg von 160 % bei kompromittierten Logins zu verzeichnen.

(1) **Kompromittierungsmethoden:**

Es sind die „Klassiker“:

- ▶ Geknackte Datenbanken
- ▶ Phishing
- ▶ Malware

und dann gehen diese Daten direkt in Open-, Deep- und Dark-Web-Foren zum Verkauf.

(2) **Schutzmethoden**

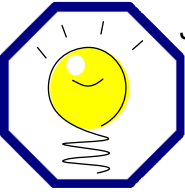
Auch hier sind es die „Klassiker“:

- ▶ Passwortrichtlinien
- ▶ Multi-Faktor-Authentifizierung
- ▶ Begrenzung der Anmeldeversuche
- ▶ Begrenzung auf erforderliche Nutzungszugänge

⁷⁵ Link: BSI: „[Wegweiser für den digitalen Alltag](#)“

⁷⁶ Quelle: SECURITY INSIDER: „[Cyberkriminelle greifen nach digitalen Identitäten. Alarmierender Anstieg ...](#)“

- Schulungen
- Technische Schutz- und Vorsorgemaßnahmen.



Je nach Ausprägung der Datenverarbeitung und der Organisation sollten diese Maßnahmen mindestens angegangen sein. Übrigens zählt dies auch zu den technischen und organisatorischen Maßnahmen des Datenschutzes.



n) Europäische Suchmaschine(n)

Wie Golem.de⁷⁷ berichtet, sind ECOSIA und QWANT mit einem eigenen, europäischen Suchindex gestartet. Bisher war man ausschließlich von US-Konzernen abhängig. Deshalb gründeten beide Firmen ein Gemeinschaftsunternehmen „EUSP“ European Search Perspektive. Die Einführung in Deutschland ist für Ende 2025 (also jetzt) angekündigt.

Bei Bedarf, einfach mal sprechen!



⁷⁷ Quelle: Golem.de: „[Ecosia und Qwant starten europäischen Suchindex](#)“

Quelle: ECOSIA BLOG: „[The Internet just got better: our European search index goes live](#)“