Übersicht 2025 | Zum Datenschutz aufgefallen

Information zum (Weblink)

Datenschutz - Service

oder Fragen per Mail an:

Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtigkeit und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männlichen Form, die alle Geschlechter mit einbezieht.

Liebe(r) Leser(in)*,

Datenschutz → einfach praktisch hilfreich!

Wenn die Grundlagen einmal gelegt, sind die Abläufe meist schlank(er), der Aufwand gering und mit (der) Sicherheit mehr Zeit gewonnen. Datenschutz schafft Vertrauen und ist eine Grundlage für nachhaltigen Erfolg.

Mein Ziel ist es, den Datenschutz einfach, praktisch und hilfreich zu vermitteln und zu gestalten. Von Datenschutzberater, Datenschutzberatung, Datenschutzmanagement bis zertifizierter, externer Datenschutzbeauftragter für Selbstständige, Gewerbetreibende und KMU.

Sprechen wir!

Vielen Dank für Ihr Interesse

PS: Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist, oder kontaktieren Sie mich gerne.

HINWEISE:

Das Inhaltsverzeichnis finden Sie ab Seite 2:

- ✔ Die Einzelthemen können Sie mit einem Mausklick in der Inhaltsangabe direkt ansteuern
- ✔ Mit der Suche <Strg + F> können Sie auch Ihr Thema direkt finden
- ✔ Die Quellenangaben können über einen Mausklick auf die Fußnote <NR.> direkt angesteuert werden.
- ✔ Letzte, integrierte Monatsinformation: März 2025

1. Standard – Datenschutz – Modell Vers. 3.1

Standard-Datenschutz-Modell *übersichtlich zusammengefasst* *11 Seiten*	**Standard-Datenschutz-Modell** Datenschutzkonferenz DSK 77 Seiten	**Datenschutz-Grundverordnung** auf dejure.org	**Bundesdaten-schutzgesetz** auf dejure.org

Das SDM [*der Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder (DSK)*] überführt die rechtlichen Anforderungen der DS-GVO über 7 Gewährleistungsziele in die technischen / organisatorischen Maßnahmen zur Unterstützung der Transformation abstrakter – rechtlicher Anforderungen in konkrete Maßnahmen. Ziel ist, eine gemeinsame Sprache der Juristen und Informatiker für die Verantwortlichen und Datenschutzpraktiker zu finden. | Aktuell: SDM Version 3.1 (05/2024) | Letzter Baustein 11/2021: Nr. 51 „Zugriff auf Daten, Systeme und Prozesse regeln“

**) Mit der Version 3.0 wird im Wesentlichen die Prüfroutine für eine Datenschutzprüfung anschaulicher und detaillierter erläutert. Die Zusammenfassung des SDM auf 11 Seiten ist auf Version 3 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).*

Monate 2025: Jan., Feb.,

Inhalt

(Einfach interessantes Thema nach Wahl anklicken)

1. Standard – Datenschutz – Modell Vers. 3.1.....1
2. Zum Datenschutz.....3
a) Löschkonzept erstellt?.....3
(1) In der DS-GVO dazu:.....3
(2) Mögliche Antworten des Verantwortlichen u/o Datenschutzbeauftragen.....3
(3) Löschkonzept (Inhalte).....3
b) Wie weit geht das Auskunftsrecht?.....3
(1) Hintergrund:.....3
(2) Die Urteile:.....3
(3) Welche möglichen Ausnahmen bestehen?...4
c) Doctolib – Gesundheitsdaten für KI-Modelle ???.....4
d) Datenschutzverletzung und Meldepflichten....5
(1) Die Meldepflicht.....5
(2) Die Datenschutzverletzung.....5
(3) Handlungsempfehlungen.....5
(3.1) Checkliste:.....5
(3.2) Risikobegrenzung / -vermeidung:.....5
3. Zur Datensicherheit.....6
a) DMA, DORA, DSA, KRITIS, CERT & NIS-2?. 6
(1) DMA – Digital-Markets-Act.....6
(2) DSA – Digital-Service-Act.....6
(3) DORA – Digital-Operational-Resilience-Act..6
(4) NIS-2 (Network-and-Information-Security)....7
(5) KRITIS – Kritische Infrastruktur (CER).....7
b) Manipulierte Rechnung per E-Mail.....7
(1) Der Fall.....7
(2) Das Urteil.....7
c) HP-Universal-Drucker-Treiber mit kritischer Sicherheitslücke (UPDATE !!!).....8
d) Sicherheitslücken – Risiko für die Guten.....8
4. Zu angrenzenden Themen.....8
a) Hält der EU US-Angemessenheitsbeschluss?8
b) Die „Dracula Suite“.....8
c) GoBD Änderung Fristen.....8
d) Supportende Windows 10.....8

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 Datenschutzbeauftragen

(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 Oldenburg[1] 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.

(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

1 *Quelle: Niedersachsen / Oberlandesgericht Oldenburg: „Zwischen Detektiveinsatz und Datenschutz ...“*

DSVGO) 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 Schutzrechte[2], 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 berichtet[3], 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 Werbeplattform Outbrain, stört mich schon der Punkt 4.2 in den Datenschutzbestimmungen[4]:

> ***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 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

2 Quelle: Gabler Wirtschaftslexikon: „gewerbliche Schutzrechte"
3 Quelle: Netzpolitik.org: „Neue Datenschutzhinweise Doctolib will KI-Modelle mit Gesundheitsdaten trainieren"
4 Link: Doctolib: „Datenschutzhinweise (PDF)"

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 Betroffen 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 Erkenntnis können zur Anpassung der technisch-organisatorischen Maßnahmen genutzt werden, um Vorfälle diese Art künftig zu vermeiden.

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-Act[5]

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-Act[6]

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 17.021.2024)*

(3) DORA – Digital-Operational-Resilience-Act[7]

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):

5 *Quelle: EU: „Gesetz über digitale Märkte“*
6 *Quelle: Europische Kommission: „Gesetz über digitale Dienste: Fragen und Antworten“*
7 *Quelle: European Insucrance and Occupational Pensions Authority: „Gesetz über die digitale operative Resilienz (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.“

(4) NIS-2 (Network-and-Information-Security)[8]

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)[9]

Ausgangsbasis ist die EU-RCE Directive bzw. die CER-Richtlinie (Critical Entites 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“[10] an.

b) Manipulierte Rechnung per E-Mail

(1) Der Fall

… vor der 2. Zivilkammer des LG Rostock[11]:

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 hätte man sich wissentlich auf die ungeschützte E-Mail-Kommunikation geeinigt, zudem wies die E-Mail eine fehlerhafte HTML-Formatierung auf, und der

8 *Quelle: Secjur.com Grafik: „KRITIS vs. NIS2-Übersicht“*
9 *Quelle: BSI: „Pflichten für KRITIS-Betreiber“; BMI: zu KRITIS-Dachgesetz; Open KRITIS: „KRITIS – auf den zweiten Blick“*
10 *Link: BSI: „Umsetzung der NIS-2-Richtlinie für die regulierte Wirtschaft“*
11 *Quelle: landesrecht-mv.de: „LG Rostock 2. Zivilkammer Aktenzeichen 2 O 450/24 vom 20.11.2024“*

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 !!!)

Heise Online[12] 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. Datenschutz[13] 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 Disclsoure“, 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.[14]
- Schlimmste Konsequenz, die Schwachstellen werden aus diesem Grund nicht mehr gemeldet und die „Bösen Hacker“ nutzen diese für ihren Betrug.

4. Zu angrenzenden Themen

a) Hält der EU US-Angemessenheitsbeschluss?

Wie Datenschutzticker.de[15] 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“[16]

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 Bürokratieentlastungsgesetz 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 10[17]

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

12 *Quelle: heise online: „Alert: HP: Kritische Lücken in Universal-Druckertreiber ermöglichen Codeschmuggel“*
13 *Quelle: Dr. Datenschutz (intersoft consulting services): „Meldung von Sicherheitslücken – Risiko für die „Guten“*
14 *Quelle: inside digital: „Hacker-Skandal: CDU verklagt Sicherheitsforscherin, die gravierende Lücke entdeckt hat“*
15 *Quelle: datenschutzticker.de: „EU-US-Datenschutzrahmen durch Trump bald Geschichte?“*
16 *Quelle: chip.de news/cyber-security. „Experten schlagen Alarm: Gefährliches Tool macht Betrug einfacher denn je“*
17 *Quelle: SECURITY-INSIDER: „Alles was Sie über das Ende von Windows 10 wissen müssen“*

Kriminelle zu werden, da keine Sicherheitsupdate mehr zur Verfügung gestellt werden.

(1) Alternative: Umstieg auf Windows 11

(2) Windows 10 mit kostenpflichtigem ESU–Service[18] 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 0Patch[19], 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.

Bei Bedarf, einfach mal sprechen! 

18 *Link: Microsoft: „Esu-Programm (Extended Security Updates) für Windows 10“*
19 *Link: 0patch Blog: „Long Live Windows 10... With 0patch “*