# Dezember 2022 | 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 der Grundlagen 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.***

## Inhalt

*(Einfach interessantes Thema nach Wahl anklicken)*



## 1. Standard – Datenschutz – Modell Vers. 2.0b

Das SDM [der Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder (DSK)] überführt die rechtlichen Anforderungen der DS-GVO über 7 Gewährleistungsziele in die geforderten technischen und 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.

| | | | |
|---|---|---|---|
| | **Zusammenfassung SDM (10 Seiten)** | | Link DS-GVO auf dejure.org |
| | Link zum SDM der Aufsicht (72 Seiten) | | Link BDSG auf dejure.org |

***Letzte Ergänzung: 11/2021: Baustein 51 (zu TOM)***

Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln" (V.1.0 / 01.11.2021 / 23 Seiten)[1]. Kurze Zusammenfassung (1. Seite) und ein Richtlinienentwurf (2. Seiten), falls wünschenswert[2].

Sorry! Am 24.12.2022 teilt die DSK mit, dass eine neue Version 3.0 veröffentlicht wurde. Nach einem Überflug sind es Vereinfachungen und Verschlankungen. Dazu demnächst dann mehr.

## 2. Zum Datenschutz

### *(a) Datenschutzverletzung*

Nach Art.33 DS-GVO muss die Verletzung zu schützender, personenbezogener Daten innerhalb von 72 Stunden durch den Verantwortlichen an die zuständige Aufsichtsbehörde gemeldet werden, wenn dies voraussichtliche zu einem Risiko für die natürlichen Personen führt. Der Auftragsverarbeiter hat dies unverzüglich an die Verantwortlichen zu melden(!).

1 *Quelle: SDM – Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln" der DSK (23 Seiten)*
2 *LINK: Kurze Zusammenfassung Baustein 51: Zugriffe auf Daten, Systeme, Prozesse (1 Seite ) & Richtlinienentwurf (2 S.)*

### *i) „Kleine Fische“ gibt es nicht*

In der NZZ ist ein kurzweiliger Bericht[3] einer Gesellschaft mit 20 Mitarbeitern. Nur so viel, dank der Sicherheitslösungen kam es zu keiner Verschlüsselung, allerdings tauchten im Darknet interne Dokumente auf und es waren Daten von tausenden Kunden betroffen (Admin: „ Stresstest“).

### *ii) Dokumentation | Meldung | Information*

Eine kurze Übersicht gibt die Website der LfDI-NRW zu den Pflichten bei einer Verletzung[4].

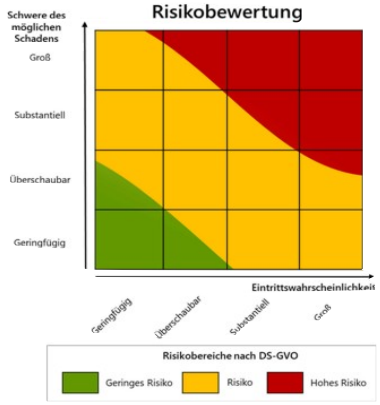
- Interne Dokumentationspflicht: kein bis geringes Risiko (also immer)
- Meldepflicht an Aufsichtsbehörde: mittleres Risiko
- Betroffenen – Information: hohes Risiko

Oft genannte Beispiele für kein bis geringes Risiko sind der Verlust einer nach dem Stand der Technik verschlüsselten Festplatte, zu der ein Backup besteht, oder veröffentlichte (z.B. Telefonbuch, Website), bekannte E-Mail- oder Adressdaten u. ä.

### *iii) Risikoanalyse*

Grundsätzlich hat eine Risikoanalyse aus Eintrittswahrscheinlichkeit und möglicher Schwere eines Schadens zu erfolgen, wie hier rechts im Bild gezeigt. Hinweis (übrigens):

> *„Es ist NICHT ZULÄSSIG auf Anforderungen der Grundsätze nach Art. 5 DS-GVO zu verzichten und Risiken daraus in Kauf zu nehmen. RISIKO - AKZEPTANZ oder RISIKO - TRANSFER (z. B. bekannt aus der Informationssicherheit) stehen den Verantwortlichen im Datenschutz NICHT ZUR VERFÜGUNG.“*




*Bildquelle: Datenschutzkonferenz (DSK) Kurpapier Nr. 18, Schaubild Seite 5*

Nach Art der Daten (Adressen, E-Mail, Fotos, Benutzername, Passwort, Biometrie, Berufsgeheimnis, Standort, Bank/Kreditdaten, Gesundheit, Religion, Sexualität, Politik u. ä.) ist der mögliche Schaden für die Betroffenen einzuschätzen (Finanzieller Art, Identitätsdiebstahl, Ruf- / Image-schaden, Bloßstellung, Geheimnisoffenbarung, Existenzgefährdung u. ä.).

### *iv) Was ist zu tun?*

(a) Im Vorfeld sollte neben den Schulungen zur Sensibilisierung die Meldekette festgelegt sein, die Zusammensetzung des Notfallteams incl. Datenschutzverantwortliche, -berater und mögliche, notwendige, externe Spezialisten, sowie Kommunikationsverantwortliche.

(b) Durch technische und organisatorische Maßnahmen den Schaden analysieren, eingrenzen, abschätzen und das Risiko möglichst mindern.

(c) Geeignete Information der Mitarbeiter (einheitliches Außenbild), der Aufsichtsbehörde, der Cybereinheit der Polizei und der Betroffenen. *(Wenn die Möglichkeit besteht, dass Daten in die falschen Hände geraten könnten, sollten m. E. auch bei geringem Risiko die Betroffenen informiert werden, allein um möglich Risiken besser einzuschätzen und bevor Betroffene es aus dritter Hand erfahren.)*

### *v) Vorbereitung / Checkliste Schadensmeldung*

Natürlich verweisen die meisten Websites der Datenschutzbeauftragten auf ihr Meldung im Online-Portal. Welche Informationen sie sich zurechtlegen sollten finden Sie auf meinem PDF-Formular[5]. Einfach öffnen und ausfüllen als Vorlage, oder als Meldung per Brief / E-Mail.

### *(b) MS 365, jetzt wird es spannend!*

Die Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder hat eine zusammenfassende Stellungnahme zu „Microsoft-Onlinedienste“ am 24.11.2022 nach 2-jähriger Prüfung und Abstimmungen mit Microsoft veröffentlicht[6].

✖ Schwierigkeiten bei der Rechenschaftspflicht der Verantwortlichen, mangels vollständiger Offenlegung der einzelnen Verarbeitungen.

3 *Quelle: NZZ: „Die Erpressung landet im Spam-Ordner. Tausende von Kundenadressen im Darknet: Ein Kleinunternehmen gibt einen seltenen Einblick in einen Hack“*
4 *Quelle: LfDI-NRW: „Meldepflicht für Verantwortliche – Verletzung des Schutzes personenbezogener Daten“*
5 *LINK: https://volkerschroer.de/DSGVO/Schutzverletzung.Meldung.Art.33.pdf*
6 *Quelle: DSK: https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf*

- ✖ Die Verwendung zu eigenen Zwecken als Auftragsverarbeiter schließt die Verwendung im öffentlichen Bereich (Schulen, Behörden) aus, ein berechtigtes Interesse zählt hier nicht.
- ✖ Offenlegung auch ohne Rechtshilfeabkommen mit der EU in einem Drittland möglich.
- ✖ Löschfristen können nur zu Zwecken von Microsoft verlängert werden.
- ✖ Eingeschränkte Kontrollrechte bei der Einschaltung von Unterauftragsverarbeitern
- ✖ Neben der Übermittlung in die USA (schon sehr kritisch nach den Schrems – Urteilen des EuGH), behält sich Microsoft auch die Übermittlung an Auftragsverarbeitern in andere Drittländer generell vor.

Fazit: **Die DSK bleibt kritisch zum Einsatz von MS 365!**

Wie sich Thüringens Landesdatenschutzbeauftragter in der Süddeutschen Zeitung äußerte, kann MS365 weder in Behörden, Schulen noch der freien Wirtschaft datenschutzkonform eingesetzt werden. *„Allerdings wolle er nun zunächst herausfinden, wie stark sie in der Unternehmerschaft verbreitet ist und unter anderem mit der Industrie- und Handelskammer über die Auswirkungen des Beschlusses sprechen.“*

## 3. Zur Datensicherheit

### *(a) Es wird schlimmer (Cybersecurity Report `23)*

Nach einer Analyse von 25 Mrd. E-Mails im Zeitraum 01.10.21 bis 20.09.22 stellt der Cybersecurity Report 2023 der Hornetsecurity[7] fest: Bereits knapp 41 % der E-Mails sind unerwünscht. Phishing ist mit einem Anteil von knapp 40 % die größte Angriffsart. Bei den Dateianhängen führen Archive mit 28 %, knapp gefolgt von MS-Office-Dokumenten (Word, Excel) mit 23 %.

#### *i) Trügerische Sicherheit von MS365*

*„Microsoft 365 (Markos im Standard deaktiviert) erleichtert die Freigabe von Dokumenten, jedoch bedenken Endnutzer oft die Konsequenzen für die IT-Sicherheit nicht. Hornetsecurity fand in einer Umfrage heraus, dass 25 % der Befragten entweder unsicher waren oder davon ausgingen, dass Microsoft 365 immun gegen Ransomware - Bedrohungen sei. (Zitat)*

#### *ii) „Brand Impersonation“*

… oder Diebstahl mittels geklauter Identitäten. Mit auf Social-Media-Plattformen angeeigneten Informationen über Social Engineering an Unternehmensdaten zu kommen. Zitat:

*„So stieg der Anteil von LinkedIn an den weltweit entdeckten Bedrohungen durch Brand Impersonation auf 22,4 %, was einem Anstieg von 3,5 % gegenüber dem Vorjahr entspricht.“*

## 4. Zu angrenzenden Themen

### *(a) Hackerangriffe auf Handys nehmen stark zu*

Wie die zeit-online aus einer dpa – Meldung berichtet[8], nehmen die Hackerangriffe mit zunehmender Verbreitung von Bezahl-Apps nach einer US-Analyse (Lexis Nexis Risk Solution) stark zu. *„Die EU-Zahlungsrichtlinie PSD2 und die damit verbundene Verschärfung der Login-Vorschriften habe Online-Zahlung und Überweisungen zwar sicherer gemacht, aber nicht narrensicher.“* Beispiel sind die in Not geratenen Angehörigen, was dringend einer Überweisung bedarf u. ä.

### *(b) Aufpassen wie ein Luchs*

Die Sicherheitsstandards sind recht hoch, auch durch die 2-Faktor-Authentifizierung u. ä. Bei den aller meisten, gelesenen „Hacks“ geht es nur noch über den „verleiteten“ Nutzer, dafür werden keine Kosten und Mühen gescheut. Also: „Aufpassen wie ein Luchs!“

**Bei Bedarf, einfach mal sprechen!**

7 Quelle: Hornetsecurity: „OUT NOW: Cybersecurity Report 2023“
8 Quelle: Zeit-Online: „Cyber-Report: Hackerangriffe auf Handys nehmen stark zu“