September 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 Richtig- und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männliche 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].

2. Zum Datenschutz

(a) Aufsicht prüft Absicherung von E-Mail-Accounts[3]

Zur eigenen Absicherung lohnt es für Verantwortliche, sich mit dem Thema auseinander zu setzen, auch wenn die Prüfung zunächst nur stichprobenartig durch die Aufsicht in Bayern erfolgt. Aufgrund ihrer Befugnisse nach Art. 58 DS-GVO nimmt die Aufsicht eine Präventionsprüfung vor.

„Seit mehreren Monaten können wir ein verstärktes Aufkommen von Cyberattacken auf E-Mail-Accounts von Verantwortlichen … Die eigentlichen Ursachen solcher Cyberangriffe sind nicht selten in einer unsachgemäßen Bedienung (u. a. aufgrund mangelndem Sicherheitsbewusstsein bei den Beschäftigten) oder in einer fehlerhaften Konfiguration und Absicherung der E-Mail-Accounts … Diesen kann jedoch ak-

Am 01.10.2022 hatte das “Amt“ etwas Schwierigkeiten mit dem Dateiaufruf

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.)*
3 *Quelle: LDA-Bayern: „Datenschutzprüfungen, E-Mail Account Absicherung“*

tiv mit vertretbarem Aufwand entgegengewirkt werden, um die drohenden hohen Schäden – wirtschaftlich wie datenschutzrechtlich – … gering zu halten oder im Idealfall ganz zu vermeiden.“

i) Der Antwortbogen[4]

… enthält fünf Aussagen, die mit „Ja“ oder „Nein, nicht / teilweise (Begründung ist beizufügen)“ zu beantworten sind (Kurzform):

1. Phising – Awerness und allgmeines Sicherheitsbewusstsein
   Werden Mitarbeiter/-innen regelmäßig und passend zu öffentlich bekannten Bedrohungslagen und E-Mail – Angriffsarten in geeigneter Weise geschult?
2. Passwörter, Mehr – Faktor – Authentifizierung und Benutzerverwaltung
   Besteht ein Rollen- und Berechtigungskonzept nach dem Erforderlichkeitsprinzip, Zugangspasswörter mit ausreichender Komplexität und besonders schützenswerte Bereiche mit Mehr – Faktor – Authentifizierung bei regelmäßiger Rechteüberprüfung?
3. Administrative Pflege und Konfiguration der E – Mail – Konten
   Erfolgt die Verwaltung der Postfächer in strukturierter Form durch eine Fachkraft / -abteilung / Dienstleister? Sind die Einstellungen gezielt konfiguriert, abgesichert und werden regelmäßig überprüft (Änderung „Default“)? Werden Sicherheitseinstellung für Weiterleitung, Abwesenheit und Onlinezugang berücksichtigt?
4. Überprüfung Datenverkehr
   Werden Aktivitäten auf bekannte, schadhafte Zugriffe kontrolliert, blockiert und sind mit Alarmhinweis versehen? Besteht ein Protokollierungs- und Analysekonzept (Umgang mit Störungsmeldungen, Manipulationsschutz u.s.w.)?
5. Device und Patch Management sowie Backup – Konzept
   Besteht eine Inventarübersicht aller IT-Komponenten und eingesetzter Software mit Sicherheitsvorgaben zu Einstellungen und Verwendung? Besteht ein Update und Backup – Konzept mit regelmäßiger Überprüfung?

ii) Detaillierte Checkliste (Handreichung)[5]

Zu den 5 Fragen werden konkrete Detail – Punkte zur Selbsteinschätzung angeführt (☐/☒).

iii) Informationsblatt[6]

(b) E – Mail – Stress

Folgt man einer Studie von SEPPMail[7] fühlt sich jeder 4. ab 29 E – Mails pro Tag gestresst und ich kenne viele, deren tägliche Mails diese Grenze weit übersteigen. Da gibt es die Gruppe der Autarken (Wichtig: Sicherheit, Manipulationsschutz) und die der Agilen (Wichtig: Erreichbarkeit, Schnelligkeit) mit unterschiedlichem Stress- und Vorsichtlevel, denn:

Je gebildeter Menschen in Sachen Cyber Security sind, desto besorgter: 60 % der geschulten MitarbeiterInnen sind aufgrund ihrer Kompetenz gestresst – weil sie die zahlreichen Angriffsoptionen kennen.

Mögliche Gegenmaßnahmen:

- Zumindest die eigenen E – Mails sollten einen aussagefähigen Betreff enthalten (INFO / AUFTRAG / NACHFRAGE / NACHTRAG u.s.w.)
- Im ersten, auf dem Bildschirm abgebildeten Absatz sollte Anlass und Auftrag ersichtlich sein. Empfänger in <cc> = „kann man lesen, oder später, oder aber muss man nicht“.
- Sensibilisierungsschulungen sind wichtig (und nicht nur vorgeschrieben).
- Erläuterung der Sicherheitsvorkehrungen (Firewall, Spam – Filter, Blacklists, Sperrungen, Absenderkontrollen u. ä.) reduziert das Stresslevel und gibt Sicherheit.
- Jederzeitige, freundliche Hilfestellung bei Zweifeln und Störungsfällen.
- E – Mail Signaturen, Verschlüsselungen oder eine Verlagerung von wichtiger Kommunikation auf „END TO END“ verschlüsselte Messanger.
- Und natürlich die Grundprinzipen: „Weniger ist mehr!“; „Fasse Dich kurz und eindeutig!“.

4 *LINK: LDA-Bayern: „Antwortbogen“*
5 *LINK: LDA-Bayern: „Handreichung bzw. detaillierte Checkliste“*
6 *LINK: LDA-Bayern: „Informationsblatt“*
7 *Quelle: SEPPMAIL: „E – Mail – Stress – Studie, Mensch vs. Maschine“*

3. Zur (IT-) Datensicherheit

(a) Mit Verantwortung am Arbeitsplatz:

- ist der Anwendungszugriff bei Abwesenheit zu sperren,
- sind Dokumente, insbesondere sensible Dokument, immer wegzuschließen und auf keinen Fall in der Öffentlichkeit zu bearbeiten,
- sind Passwörter nie unter, neben oder auf dem Schreibtisch / Monitor zu platzieren und auf keinen Fall an Dritte weiterzugeben,
- sind E-Mails stets kritisch auf Seriosität zu prüfen,
- sind öffentliche WLAN – Netze zu meiden,
- sind Unregelmäßigkeiten oder Hardwareverlust umgehend zu melden,
- und sich bei Fragen oder Unsicherheiten an die betrieblich Verantwortlichen zu wenden.

Warum? Siehe nachfolgenden Punkt 4(a).

(b) MS Windows 10 Support endet(!)

Ich musste mir erst die Augen reiben, war nicht zur Veröffentlichung für Windows 10 die „endgültige“ Betriebsversion angekündigt? Es scheint nicht so zu sein! Bei Home und Pro (Privat) in der Version 21H1 enden Updates am 13.12.2022 (dieses Jahr), bei 21H2 am 13.06.2023, bzw. Enterprise and Education (21H2) am 11.06.2024. Wer auf die Version 22H2 (z.B. im Rahmen des Windows – Insider – Programms aktualisiert hat, kann mit Updates bis 14.10.2025 rechnen.[8] Hilfreich ist sicherlich die eigene Version zu prüfen mit <⊞> + <R> und Eingabe <winver>[9]

4. Zu angrenzenden Themen

(a) Wer haftet den nun?

Wer kann bei einem Datenschutzverstoß überhaupt in Anspruch genommen werden? Diese Frage taucht in Regelmäßigkeit immer wieder auf. Zitiert werden i. d. R. die Urteile des OLG Dresden vom 30.11.2021 (AZ.: 4 U 1158/21)[10], BAG v. 05.02.2004 (AZ:8 AZR 91/03)[11] und LAG Sachsen vom 07.04.2022 (AZ: 9Sa250/21)[12]

i) Geschäftsführer / Unternehmen

Grundsätzlich haften die Verantwortlichen, die alleine oder gemeinsam über Zweck und Mittel der Verarbeitung (und deren Erhebung) personenbezogener Daten entscheiden (Art.4, Nr.7 DS-GVO). Das sind i. d. R. Geschäftsführer, Vorstände u.s.w. Nach der Entscheidung des OLG reicht es aus, von der Datenverarbeitung zu profitieren, sie zu veranlassen oder zu dulden, ohne selbst Zugriff auf, oder Verarbeitung von Daten zu haben. Im Normalfall übernimmt das Unternehmen das Bußgeld / den Schaden. Bei Missachtung des Datenschutzes / -sicherheit können auch die Verantwortlichen wegen mangelnder Organisation / Aufsichtspflicht persönlich haften.

ii) Mitarbeiter

Das Bundesarbeitsgericht unterteilt die Mitarbeiterhaftung in leichte Fahrlässigkeit ohne Haftungsfolgen (bei leichten Pflichtverstößen, Fehler können passieren), mittlere Fahrlässigkeit mit einer anteiligen Haftung (Mitarbeiter hätte Schaden voraussehen können) und grobe Fahrlässigkeit (wissentlich Schaden oder Regelverletzung in kauf genommen) mit voller Haftung bei sozialen Grenzen.

Im Fall des OLG Dresden wurde trotz mehrfachen Hinweises auf den Verstoß gegen die Informationssicherheitsrichtlinie (Clean-Desk) verstoßen, was zu einer erheblichen Pflichtverletzung führte und nach Mahnungen und Abmahnung, folgte die (rechtmäßige) Kündigung.

Bei Bedarf, einfach mal sprechen!

8 *Quelle: Microsoft: „Support dates Windows 10 Home and Pro“; „Enterprise and Education“, „Releasing WIn10 Vers. 22H“*
9 *Quelle: Microsoft: „Welche Version des Windows Betriebssystem verwende ich?“*
10 *Quelle: openjur.de: „OLG Dresden, Urteil vom 30.11.2021 - 4 U 1158/21“*
11 *Quelle: BAG v. 05.02.2004 (AZ:8 AZR 91/03): „Grundsätze der Beschränkung der Mitarbeiterhaftung“*
12 *Quelle: LAG Sachsen vom 07.04.2022 (AZ: 9Sa250/21): „Verhältnismäßigkeit Nachlässigkeit – Abmahnung – Kündigung“*