November 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.....1

Letzte Ergänzung: 11/2021: Baustein 51 (zu TOM).....1

2. Zum Datenschutz.....1

(a) Pflicht zur Benennung eines Datenschutzbeauftragten.....1

i) Grundsätzlich:.....1

ii) Die Pflicht zur Benennung:..2

iii) Fragen schadet nicht:.....2

3. Zur Datensicherheit.....2

(a) Sicherheit mit Bordmitteln…2

i) Cloud.....2

ii) Betriebssystem.....3

iii) Router / WLAN / LAN.....3

iv) Fragen schadet nicht.....3

4. Zu angrenzenden Themen.....3

(a) Aktuelle Betrugsmaschen häufen sich:.....3

i) Messenger - Betrug.....3

ii) Datenabgleich Paypal.....3

iii) Perfider DHL – Betrug.....3

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) Pflicht zur Benennung eines Datenschutzbeauftragten

i) Grundsätzlich:

Die Verantwortung, also in der Pflicht zur Einhaltung des Datenschutzes sind und bleiben immer die Verantwortlichen. Den Datenschutzbeauftragten obliegen (Art.39 DS-GVO) die Unterrichtung und Beratung der Verantwortlichen (einschl. Auftragsverarbeiter) und der Beschäftigten zur Einhaltung der Vorschriften (Abs.1a), deren Überwachung, der Zuweisung von Zuständigkeiten, sowie Sensibilisierung und Schulung (Abs.1b), der Beratung auf Anfrage bei Durchführung einer Datenschutz – Folgenabschätzung (Abs.1c), die Zusammenarbeit mit Aufsichtsbehörden (Abs.1d) und deren Anlaufstelle bei Fragen oder notwendigen Konsultationen. Dabei sind sie vollumfänglich von

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.)*

den Verantwortlichen zu unterstützen, zu informieren und frühzeitig einzuschalten (Art.38 DS-GVO).

ii) Die Pflicht zur Benennung:

Die DS-GVO enthält verschiedene Öffnungsklauseln für die Regelungen in einzelnen Mitgliedsstaaten zur Präzisierung des Art.37 DS-GVO und Klarstellung: §38 BDSG, Datenschutzbeauftragte für nicht öffentliche Stellen. Die Pflicht zur Benennung besteht:

- Wenn mindestens 20 Mitarbeiter ständig (auch nur am Rande) mit der automatisierten Bearbeitung personenbezogener Daten beschäftigt sind.

oder Wenn für die Bearbeitung eine Datenschutz – Folgenabschätzung* notwendig ist.

**) Art. 35 DSGVO bei hohem Risiko, insbesondere Art.9 besondere Kategorien, Art.10 Straftatbestände, systematische und umfassende Bewertung persönlicher Aspekte, automatisierte Verarbeitung und Profiling*

oder Wenn personenbezogene Daten (auch anonymisiert) übermittelt werden.

oder Wenn personenbezogene Daten für Markt- oder Meinungsforschung verarbeitet werden.

oder Bei Behörden, mit Ausnahme von Gerichten

oder Die Kerntätigkeit liegt in umfangreicher, regelmäßiger und systematischer Überwachung betroffener Personen (z. B. Auskunfteien, Personalabteilung, Sport- / Navigationsapps)

oder Die Kerntätigkeit liegt in der umfangreichen Verarbeitung von besonderen Kategorien (Art.9 DS-GVO) oder strafrechtlicher Daten (Art.10 DS-GVO). (z. B. ist eine einzelne Arztpraxis ausgenommen, eine Praxisgemeinschaft ggf. mit Labor nicht).

iii) Fragen schadet nicht:

Ob die Benennung eines Datenschutzbeauftragten notwendig ist, oder nicht, oder ein unsicherer Punkt zu klären ist, kann die Frage an einen oder Ihren Datenschutzbeauftragten nicht schaden.

3. Zur Datensicherheit

(a) Sicherheit mit Bordmitteln

Wer keinen Informationssicherheitsbeauftragter (ISB) beschäftigt, kann oft mit nur wenigen, einfachen Maßnahmen einen größeren Schaden verhindern.

i) Cloud

In einer Studie der Cloud Security Alliance (.org; CSA)[3] gibt es nach wie vor große Bedenken gegenüber der Cloud-Sicherheit. 62% der 1.662 Befragten gehen davon aus, dass ihre Organisation / Unternehmen im nächsten Jahr von einer Datenschutzverletzung betroffen sein wird. Die meist genutzten Clouds sind OneDrive (Microsoft) und Google Drive. Zur sicheren Übertragung wird bei beiden Anbietern eine SSL-Verschlüsselung mit AES-256 genutzt, um vor dem Zugriff Dritter zu schützen. Nach dem Praxistipp des Spiegels nebst Erläuterung[4], eine der sichersten Verschlüsselungsmethoden („Goldstandard"). Für einen Zugriff wird man am Passwort des/der Nutzer* nicht vorbeikommen. Allerdings liegen die Daten auf den Servern der Anbieter unverschlüsselt. Sicherheit mit Bordmitteln:

- Zunächst ein sicheres Passwort auswählen.
- Zwei-Fakor-Authentifizierung aktiveren über z. B. Microsoft u/o Google Authenticator, oder Drittanbieter wie Sophos-Intercept-X for Mobile[5] für alle die darauf zugreifen dürfen. *(Kein Sponsoring, Werbung o. ä., nur Beispiel)*
- Und ganz sicher vor dem Zugriff Dritter ist, die Daten vor der Übertragung selbst zu verschlüsseln, z. B. mit der Open-Source-Software Cryptomator. Für Teams gibt es hier auch den Cryptomator Hub, beides mit AES-256 Verschlüsselung[6]. *(Kein Sponsoring, Werbung o. ä., nur Beispiel)* DAS, entspricht auf jeden Fall auch der DS-GVO.

3 *Quelle: CSA: „Understanding Cloud Data Security and Priorities" (19.10.2022)*
4 *Quelle: Spiegel – Praxistipp: „AES-256: Bedeutet und Sicherheit der Verschlüsselung"*
5 *Quelle: SOPHOS: „Mobile Threat Defense for Android, iOS und ChromeOS"*
6 *Quelle: Cryptomator: „Hänge ein Schloss vor deine Cloud"*

ii) ***Betriebssystem***

Ob Windows, macOS, Linux, alle Systeme sind mit den Standardeinstellungen meist gut gerüstet. Ein prüfender Blick über die Sicherheitseinstellung kann aber nicht schaden, um sicherzugehen, dass nicht ein Hinderungsgrund (aus Vorinstallation, Installation, inkompatibler Treiber u. ä.) etwas nicht aktiviert ist. Am Beispiel Windows hat sich Security-Insider in einem Artikel vom 08.11.2022(+Video, Bildergalerie)[7] mit den (ausreichenden) Bordmitteln gegen Ransomware über das 3-Stufen-Modell beschäftigt.

Stufe 1: Aktiver Viren- und Mailware Scanner (First line of defense)

Stufe 2: Aktive Überwachung des Ordnerzugriffs zur Verhinderung einer Verschlüsselung

Stufe 3: Backup zur Wiederherstellung für den Notfall

„Zehn Maßnahmen zur Absicherung gegen Angriffe aus dem Internet“ hat das BSI[8] in einer übersichtlichen Broschüre zusammengestellt[9].

iii) ***Router / WLAN / LAN***

Kurz und übersichtlich sind auch die *„Sicherheitstipps im privaten und öffentlichen WLAN“*[10], *unter anderem:*

- *Standardpasswort und Standard - Netzwerkname ändern*
- *Aktuelle Firmware und aktiver Filter der Geräte - MAC-Adressen*
- *Langes und komplexes WLAN-Passwort (20 Zeichen, groß, klein, Zahlen, Sonderzeichen)*
- *Einrichtung eines Gast – Netzwerks für unsichere Geräte und in öffentlichen Netzwerken*
- *Ist die Firewall für den Zugang über öffentliche Netzwerke eingerichtet?(!)*
- *Einschalten, nur wenn es erforderlich ist*
- *Wenn es unvermeidbar ist, Abruf von vertraulichen Informationen über VPN.*

iv) ***Fragen schadet nicht***

Oder fragen Sie einfach ihren Techniklieferanten / IT-Dienstleister nach den eingestellten Sicherheitsfunktionen.

4. Zu angrenzenden Themen

(a) ***Aktuelle Betrugsmaschen häufen sich:***

i) ***Messenger - Betrug***

Das LKA Niedersachsen warnt vor: *„Messenger – Betrug: Die Gefahr durch gefälschte Freunde- oder Familienkontakte“* [11]. Versuche, Messenger - Nutzer mit Nachrichten davon zu überzeugen, dass sie Freunde oder Familienangehörige seien (neue Telefonnummer). Im Anschluss wurde um Verifizierungscodes und später um Überweisungen gebeten.

ii) ***Datenabgleich Paypal***

Das Phishing - Radar der Verbraucherzentrale warnt aktuell vor einer Forderung nach Datenabgleich der Paypal - Kundschaft um an Verifizierungsdaten zu kommen[12].

iii) ***Perfider DHL – Betrug***

[chip.de] Kriminelle versenden Phishing-Mails an DHL – Kunden. Wegen offener Zollgebühren (€1,89) könne ein Paket nicht ausgeliefert werden. Bezahlung über eingefügten Link[13].

Bleiben Sie wachsam, mit dem 3-Punkte-Check des BSI (Absender, Betreff, Anhang/Link)[14]

Bei Bedarf, einfach mal sprechen!

7 *Quelle: Security-Insider: „Ransomeware-Schutz mit Windows Bordmittel“*
8 *Abkürzung: „BSI“ – Bundesamt für Sicherheit in der Informationstechnik*
9 *Quelle: BSI: „Zehn Maßnahmen zum Schutz vor Angriffen aus dem Internet (PDF)“*
10 *Quelle: BSI: „Sicherheitstipps im privaten und öffentlichen WLAN“*
11 *Quelle: LKA Niedersachsen. „Messenger-Betrug: Die Gefahr durch gefälschte Freunde- oder Familienkontakte“*
12 *Quelle: Verbraucherzentrale aktuelle Warnungen: „18. November 2022: Datenabgleich von Paypal-Kundschaft gefordert“*
13 *Quelle: chip.de: „DHL-Kunden in Gefahr: Besonders perfide Betrugsmasche im Umlauf“*
14 *Quelle: BSI: „Nutzen Sie die E-Mail (Messenger) wirklich sicher?“*