Oktober 2024 | 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.

Inhalt

(Einfach interessantes Thema nach Wahl anklicken)

1. Standard – Datenschutz – Modell Vers. 3.1

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

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“

2. Zum Datenschutz & 3. Zur Datensicherheit

(a) Datensicherheit zum Datenschutz

Wie schon in Verordnung und Gesetz geregelt, muss nicht jeder, vom (Solo-) Selbständigen über KMUs bis zu „Internetgiganten“, alle weltweit möglichen Schutzmaßnahmen und Sicherheitsanwendung einsetzen. Zur „Sicherheit der Verarbeitung“ führt Art.32 DSGVO aus:

„(1) Unter Berücksichtigung des Stands der Technik,“

- Die Technik sollte schon dem aktuellen Niveau entsprechen.

„… der Implementierungskosten“

- Die Kosten sollen sich in einem angemessenen Rahmen zu den verarbeiteten Daten bewegen und müssen nicht überborden.

„… und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung“

- Je größer Art, Umfang und Zweck, zum Beispiel große Mengen an Daten verteilt über eigene, Rechenzentren, Dienstleister, Cloud und verteilt über Landesgrenzen erfordern

höhere Schutzmaßnahmen und damit Kosten, als ein eigener, einzelner Client bzw. Rechenzentrum.

„... sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“

- Hiermit ist der besondere Schutz für besondere Kategorien personenbezogener Daten nach Art.9 DSGVO gemeint. Daneben sind auch beispielhaft Daten zum Identitätsdiebstahl oder dem Kontozugriff gemeint oder der Verlust wichtiger Daten für die betroffene Person. Alle Daten, die ein hohes Schadensrisiko bei Verlust für den betroffenen bedeuten. Das kann dann auch höhere Aufwandskosten zum Schutz bedeuten.

... treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; ...

- Zu den organisatorischen Maßnahmen gehört der räumliche Schutz der Verarbeitungstechniken, z. B. Zutrittsberechtigungen, Schutz vor Feuer, Wasser und technischem Ausfall. Die Mitarbeiter sind zur Einhaltung zu verpflichten (Datenschutzrichtlinie), zu informieren (Merkblatt & Information) und regelmäßig über die Schutzmaßnahmen und Gefahren mindestens durch jährliche Schulungen zu sensibilisieren.
- Zu den technischen Maßnahmen gehören eine ausreichende Belastbarkeit der Systeme zur Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit, sowie Wiederherstellung nach einem Zwischenfall. Außerdem sollte eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit erfolgen.

(b) Geeignete technische Maßnahmen zur Datensicherheit?

Zur Auswahl von geeigneten technischen Maßnahmen stellt das Bundesamt für Sicherheit in der Informationstechnik verschiedene Stufen zur Cybersicherheit zur Verfügung.

i) Leichter Einstieg (KMUs)[1]

BSI: „In Zeiten der Digitalisierung kommen auch kleine und mittlere Unternehmen nicht umher, sich in Sachen Cyber-Sicherheit weiterzuentwickeln.“ (Basiselemente)

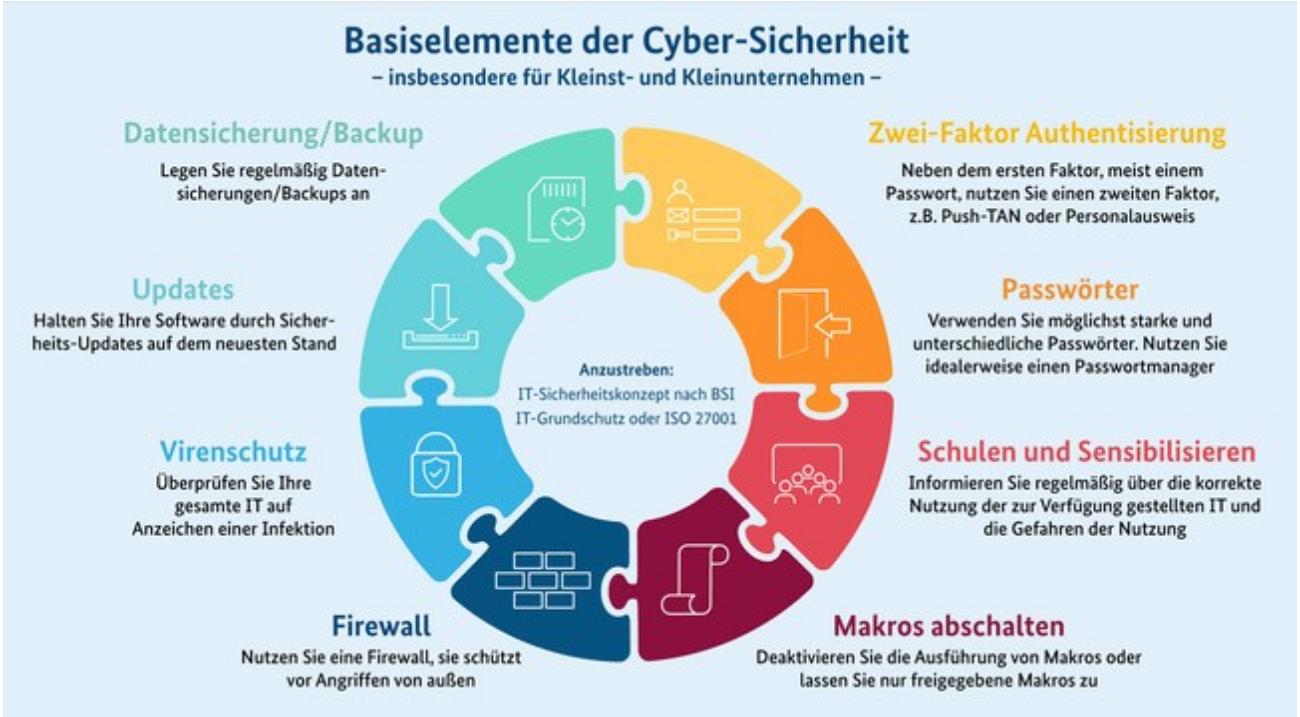

Schaubild: Quelle: Bundesamt für Sicherheit in der Informationstechnik

Eine zusammenfassende Erläuterung der Basiselemente zum Einstieg in die Cyber-Sicherheit für kleine Unternehmen, Selbstständige und Interessierte stelle ich hier kurz auf 6 Seiten zur Verfügung: https://volkerschroer.de/DSGVO/BSI.Einstieg.Cybersicherheit.pdf

1 *BSI: „Leichter Einstieg“*

ii) BSI IT-Grundschutz (mit Branchenprofilen)

Das BSI hat über 25 Jahre einen oder den IT-Grundschutz[2] entwickelt und entwickelt diesen nach dem Stand der Technik weiter. Der IT-Grundschutz ist praxisnahe im modularen Bausteinsystem zu allen relevanten Themen aufgebaut und bietet konkrete Sicherheitsanforderungen nach entsprechenden Branchenprofilen. Aus einer Schulung zum Basiswissen BS / IT-Grundschutz habe ich hier eine kurze und knappe Zusammenfassung (Management-Information) zusammengestellt: https://volkerschroer.de/DSGVO/BSI.Basiswissen.IT-Grundschutz.pdf.

(c) 5 & 6 von 6 einfachen Schritten zum Verzeichnis der Verarbeitungstätigkeiten

i) Schritt 5 (Datensicherheit)

Sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Umstände (Umfang, Zweck, Betroffenenrisiken) geeignete technische und organisatorische Maßnahmen für ein angemessenes Schutzniveau gewährleistet (Datensicherheit)?

E.) Sicherung der Verfügbarkeit, Vertraulichkeit und Integrität	
je-weils	O = organisatorische Maßnahmen | T = technische Maßnahmen | I = Betroffene informiert
T.)	<Zentral gesteuerte Firewall und Virenscanner>
O.)	<Unternehmensweite Mitarbeiterrichtlinie zum Datenschutz und Datensicherheit>

Einfach in Tabelle- oder Textdokument kopieren und sammeln 😉.

ii) Schritt 6 (Verzeichnis zusammenstellen)

Formvorschriften für das Verzeichnis der Verarbeitungstätigkeiten nach Art.30 DSGVO und BDSG.

„Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.“ (ErwGr: (82) DSGVO)

Dazu ist eine:

➔ Dokumentation in schriftlichem oder auch in elektronischem, unterzeichnetem Format (Abs.3), mit Name und Kontaktdaten von Verantwortlichen, sowie ggf. Datenschutzbeauftragten (Abs.1a).

➔ Diese Daten sind mit Kopien von Schritt 1 bis 5 (A bis E) zu ergänzen, da bereits enthalten:

- ✔ Beschreibung von Zweck und Kategorien der Personen & Daten der Verarbeitung (Abs.1b,c).
- ✔ Wer erhält Daten (interne & externe Empfänger in Europa, Drittland, intern. Organisation)
- ✔ und ist die Einhaltung der Datenschutzvorschriften (ex EU) gewährleistet. (Abs.1d,e i.V.m.Art.49).
- ✔ Wenn möglich, vorgesehene Löschfristen und eine allgemeine Beschreibung der technisch – organisatorischen Schutzmaßnahmen nach Verhältnismäßigkeit und dem aktuellen Stand der Technik (Abs.1f,g i.V.m. Art.32).
- ✔ Die gleichen Angaben sind für Auftragsverarbeiter (Dienstleister) zu dokumentieren (Abs.2).
- ✔ Rechtsgrundlage der Verarbeitung (§70 Abs.1 Nr.7 BDSG).
- ✔ Alternativ zu Löschfristen die Überprüfungstermine zur Notwendigkeit (Abs. 1 Nr.8).

Dokumentation Datenschutz und -sicherheit,

➢ *Sinnvolle Ergänzungen sind* Datum der Erstellung und Änderung, Art und Transparenz von Einwilligungen, Aufstellung der Auftragsverarbeiter, Sensibilisierung der Mitarbeiter, Einhaltung von Betroffenenrechten, den Umgang mit Meldepflichten, Schutzverletzung und von Risikoeinschätzungen.

➢ „Schön schreiben“ kann man es natürlich auch (z. B. Link zu Erläuterung und Muster).

Bei Bedarf, einfach mal sprechen!

2 BSI: *„IT-Grundschutz, Informationssicherheit mit System“*