August 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) Whistleblower und Datenschutz

Das Bundeskabinett hat Ende Juli das Hinweisgeberschutzgesetz (HinSchG) verabschiedet. Die Beratung im Bundestag erfolgt nach Stellungnahme durch den Bundesrat.[3] Eine EU – Richtlinie existiert bereits seit 23.10.2019[4], mit verpflichtender Umsetzung in nationales Recht bis 17.12.2021, was in der vorgehenden Regierungskoalition an der CDU gescheitert ist und jetzt umgesetzt wird. Das Hinweisgeberschutzgesetz ergänzt bestehende, gesetzlichen Regelungen (Geldwäsche, Kreditwesen, Wertpapiere, Versicherung, Börse, Wirtschaftsprüfung, Marktmiss-

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: BMJ Pressemitteilung: „Hinweisgeberschutzgesetz vom Kabinett beschlossen“*
4 *Quelle: EU: „Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019“*

brauch, Verkehr, nationale Sicherheitsinteressen, Verschwiegenheits- und Geheimhaltungspflichten u. ä.).

i) Hinweisgeberschutzgesetz (HinSchG)

Ziel von EU-Richtlinie und Gesetz ist eine bessere Durchsetzung des Rechts in Deutschland und Europa zum Schutz von Leben, Leib, Gesundheit, Beschäftigten und / oder ihrer Vertretungsorgane. Mit den Mindeststandards soll ein hohes Schutzniveau für Personen erreicht werden, die im Zusammenhang mit ihrer beruflichen Tätigkeit (Arbeitnehmer*/innen, Beamte*/innen, Selbstständige, Anteilseigner*/innen oder Mitarbeiter*/innen von Lieferanten) Informationen über Verstöße erlangen und diese melden.

Neben externen Meldestellen beim Bundesamt für Justiz (neu und bundesländerübergreifend), der BaFin, dem Kartellamt und der Finanzämter, ist jedes Unternehmen ab 50 Mitarbeitern verpflichtet, ein unabhängiges, internes Meldesystem zu installieren (ob gemeinschaftlich bis 249 MA, im Konzern oder über externe Dritte). In engen Grenzen (§§ 32ff HinSchG) ist auch eine Veröffentlichung (Offenlegung) möglich. Schadenersatzanspruch kann durch Benachteiligung des Hinweisgebers entstehen (aber auch für unredliche Hinweisgeber, bei grob fahrlässigen, unrichtigen Meldungen). Es gilt die Umkehr der Beweislast durch den Arbeitgeber, dass kein Zusammenhang besteht. Für das interne Meldesystem bestehen Informationspflichten (Eingangsbestätigung nach 7 Tagen, Statusbericht nach spätestens 3 Monaten an den Hinweisgeber) und eine Dokumentations- bzw. Berichtspflicht. Es gilt ein Ausschluss der Verantwortlichkeit für Informationen, die zur Weiterleitung notwendig sind und einem rechtlich einwandfreiem Zugriff des/der Hinweisgeber unterlagen.

ii) Schutz der Personendaten

Das Vertraulichkeitsgebot (§§ 8, 9 HinSchG): *„Informationen über die Identität einer hinweisgebenden Person oder einer Person, die Gegenstand einer Meldung ist, sollen nur in Ausnahmefällen herausgegeben werden dürfen, etwa in Strafverfahren auf Verlangen der Strafverfolgungsbehörden.(Gesetzliche Ausnahmen: Straf- und Bußgeldverfahren, gerichtliche Entscheidungen, BaFin, Bundeskartellamt, bei Erforderlichkeit zur Ergreifung von Folgemaßnahmen und bei Einwilligung).“*

iii) … im Datenschutz

Eine gute Vorlage ist die Orientierungshilfe zu Whistleblower-Hotlines der Datenschutzkonferenz der Aufsichtsbehörden (DSK) aus Ende 2018[5]. Zur Einordnung nach den Vorschriften zum Verzeichnis der Verarbeitungstätigkeiten (Erläuterung Fußnote[6]):

- ***Grund, Art, Zweck der Verarbeitung:***

  Beschäftigte in der Organisation nehmen Missstände oftmals als erste wahr und können durch ihre Hinweise dafür sorgen, dass Rechtsverstöße aufgedeckt, untersucht, verfolgt und unterbunden werden. Für diese Verantwortung verdienen sie Schutz vor Benachteiligungen (Repressalien), die ihnen wegen ihrer Meldung drohen oder sie davon abschrecken können.

- ***Zugriff, wer verarbeitet die Daten:***

  Nur unabhängige, mit der Aufgabe betraute fachkundige Mitarbeiter* (§ 15 HinSchG; Liste).

- ***Betroffene Personen und personenbezogene Daten (-Kategorien):***

  Alle natürlichen Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld der beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese melden.

- ***Rechtsgrundlage, Löschfristen, Besonderheiten:***

  Eine rechtliche Verpflichtung nach dem HinSchG (Art.6 Abs.1c DSGVO) besteht zur Datenlöschung nach der regelmäßigen Verjährungsfrist von 3 Jahren (§ 195 BGB mit Besonderheiten zu Empfängern, Transfer, Drittland)

- ***Schutzkonzept:***

  Aufgrund des hohen Schadenspotentials für den Betroffenen sind zum bestehenden Schutzkonzept (TOM) umfangreiche Schutzmaßnahmen zur deutlichen Reduzierung der Ein-

5 *Quelle: DSK: „Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines“ (PDF)*
6 *Hinweis: V. Schroer: „Zusammenfassende Erläuterung zum Verzeichnis der Verarbeitungstätigkeiten“*

trittswahrscheinlichkeit getroffen (z. B. strenges Berechtigungskonzept, separate, Systemumgebung, 2FA, Pseudonymisierung / Anonymisierung u. ä.).

PS: Das Schutzkonzept sollte die Eintrittswahrscheinlichkeit deutlich reduzieren. Bei unverändert hohem Risiko (Schadenpotential x Eintrittswahrscheinlichkeit) ist eine Vorstellung bei der Aufsichtsbehörde vorab vorzunehmen (Art.36 DS-GVO; zur Risikoabwägung siehe Fußnote[7], Zusammenfassung SDM, Seite 7).

(b) Werber & Adresshändler gemeinsam verantwortlich

Die Aufsichtsbehörde (LfDI) Rheinland – Pfalz stellt in Ihrem Tätigkeitsbericht 2020 die gemeinsame Verantwortlichkeit von Werbenden und Adresshändlern fest, *„da das werbende Unternehmen nicht selbst über die personenbezogen Daten“* verfügt. (Seite 35 Punkt: 5.3)[8]

3. Zur (IT-) Datensicherheit

(a) Multi-Faktor-Authentifizierung wirkt!

Schützen Sie alle (mindestens wichtigen) Anwendungen und Apps mit einer Multi-Faktor-Authentifizierung (MFA, z.B. Benutzer/Passwort + Authenticator auf Zweitgerät), es wirkt. Ein Bericht von Europol zeigt, dass die Multi-Faktor-Authentifizierung (MFA) Cyberattacken effektiv abwehren kann. Im konkreten Fall gaben die Hacker angesichts der MFA ihren Ransomware-Angriff einfach auf, so it-daily.net.[9] (BSI erklärt 2 Faktor Authentifizierung)

(b) Cloud, einfach verschlüsselt und synchronisiert

Wie einfach (und günstig) eine Ende – zu – Ende Verschlüsselung in der Cloud mit einem Austausch zwischen verschieden Geräten / Standorten funktionieren kann ist auf golem.de nachzulesen[10]. Mit der Verschlüsselungssoftware liegen die Daten verschlüsselt in der Cloud. Zum Bearbeiten wird eine virtuelles, unverschlüsseltes Laufwerk auf dem eigenen Gerät erzeugt. Schließt man das virtuelle Laufwerk, werden die Daten verschlüsselt und in der Cloud abgelegt. Eine Anleitung zum Nachlesen.

4. Zu angrenzenden Themen

(a) Projekt „No More Ransom“ ohne Zahlung entriegeln

Wir alle wissen, je mehr Lösegeld gezahlt wird, desto attraktiver ist ein Angriff für Kriminelle. Mit dem Angebot des Projektes „NoMoreRansom“[11] konnten mehr als 1,5 Millionen Opfern geholfen werden. Dadurch wurden Lösegeldzahlungen in Höhe von ca. € 1,5 Milliarden verhindert (ZDNET).[12]

(b) Zweifel? Phishing Mail

Die Verbraucherzentrale NRW veröffentlicht aktuell im Umlauf befindliche Betrugsmails und nimmt zur Prüfung verdächtige E-Mails an und veröffentlicht diese bei Betrugsversuch.[13]

(c) Wichtiges Update Apple Produkte!

Apple warnt vor schweren Sicherheitslücken bei iPhones, iPads und Macs: Laut Apple könnten Hacker die volle Kontrolle über die Geräte erlangen. Sicherheitsexperten empfehlen ein umgehendes Update.[14] In verschiedenen Beiträge wird berichtet, dass die Auto-Update-Funktion hier nicht greift und das Update unverzüglich vorzunehmen ist (Apple-Anleitung). Deshalb habe ich den Hinweis hier aufgenommen.

Bei Bedarf, einfach mal sprechen!

7 *Hinweis: V. Schroer: „Zusammenfassung Das Standard - Datenschutz - Modell | Management – Info“*
8 *Quelle: LfDI – RP: „Tätigkeitsbericht zum Datenschut 2020, Seite 35 Nr. 5.3“*
9 *Quelle: it-daily.net: „Multi-Faktor-Authentifizierung: Hacker geben einfach auf“; BSI erklärt 2 Faktor Authentifizierung*
10 *Quelle: golem.de: „Endlich ist unsere Cloud Ende-zu-Ende-verschlüsselt“*
11 *Link: NoMoreRansom: „Brauchen Sie Hilfe zum Entriegeln Ihres digitalen Lebens, ohne dabei Lösegeld zu zahlen*?“*
12 *Quelle: ZDNET: „Ransomware: 1.5 million people have got their files back without paying the gangs. Here's how“*
13 *Quelle: verbraucherzentrale: „Phishing-Radar: Aktuelle Warnungen“*
14 *Quelle: tagesschau.de: „Apple warnt vor Sicherheitslücke“*