Mai 2023 | 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. 3.0

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 (11 Seiten)		Link DS-GVO auf dejure.org
	Link zum SDM der Aufsicht (77 Seiten)		Link BDSG auf dejure.org

Letzte Ergänzung: 12/2022: SDM Version 3.0*

Letzter Baustein 11/2021: Nr. 51 „Zugriff auf Daten, Systeme und Prozesse regeln“

**) Mit der Version 3.0 wird im Wesentlichen die Prüfroutine für eine Datenschutzprüfung anschaulicher und detaillierter erläutert. Die Zusammenfassung des SDM auf 11 Seiten ist auf Version 3 angepasst. Anspruch mit der Ergänzung ist eine verständliche und anschauliche Standardanleitung zur Planung, Umsetzung und regelmäßigen (Über-) Prüfung für die Verantwortlichen. In Folge auch für die Datenschutzbeauftragten und Aufsichtsbehörden, möglichst sogar europaweit (so der Ansatz).*

2. Zum Datenschutz

(a) Whistleblower und Datenschutz (jetzt doch)

Die Umsetzungspflicht aus der EU – Whistleblower – Richtlinie (EU-Richtlinie 2019/1937[1]) hätte bis zum 17.12.2021 in lokales Recht umgesetzt werden müssen. Das Bundeskabinett ist dem im ersten Halbjahr 2022 mit dem Hinweisgeberschutzgesetz (HinSchG)[2] nachgekommen, zunächst

1 Quelle: EUR-Lex: „Richtlinie (EU 2019/1937) des EU-Parlaments und des Rates vom 23. Oktober 2019“
2 Quelle: Bundesministerium der Justiz: „Gesetz für einen besseren Schutz hinweisgebender Personen ...“

aber im Bundesrat gescheitert. Verabschiedet wurde es dort jetzt im Mai 2023[3] und tritt 4 Wochen nach Veröffentlichung im Bundesgesetzblatt in Kraft (Juni/Juli 2023). Das Hinweisgeberschutzgesetz ergänzt bestehende, gesetzliche Regelungen (Geldwäsche, Kreditwesen, Wertpapiere, Versicherung, Börse, Wirtschaftsprüfung, Marktmissbrauch, Verkehr, nationale Sicherheitsinteressen, Verschwiegenheits- und Geheimhaltungspflichten u. ä.).

Ziel 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.

i) Whistleblower (Hinweisgeber)

Hinweisgeber sind natürliche Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer *beruflichen Tätigkeit* Informationen über Verstöße erlangt haben und diese an die nach diesem Gesetz vorgesehenen Meldestellen melden oder offenlegen (§1 HinSchG). Für die Informationsbeschaffung besteht ein Ausschluss der Verantwortlichkeit (§36 HinSchG). Die Informationen dürfen allerdings nicht unter einem eigenständigen Straftatbestand beschafft worden sein. Falschinformation sind schadenersatzpflichtig.

ii) Schutz des Hinweisgebers

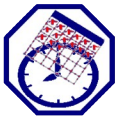
Nach dem Vertraulichkeitsgebot in den §§8, 9 HinSchG ist die Identität des Hinweisgebers zu wahren. Ausnahmen bestehen ausschließlich für Straf- und Bußgeldverfahren, gerichtliche Entscheidungen, BaFin, Bundeskartellamt und bei Erforderlichkeit zur Ergreifung von Folgemaßnahmen und bei Einwilligung.

iii) Meldestellen

Unternehmen und Organisationen ab 50 Beschäftigten müssen sichere, interne Hinweisgebersysteme installieren und betreiben. Die Organisation der Meldestelle kann nach §14 HinSchG auch an Dritte ausgelagert werden (die Verantwortung bleibt bestehen). Daneben gibt es externe Meldestellen beim Bundesministerium der Justiz, BaFin, Kartellamt, Finanzämter u.ä.).

iv) Meldungen

Es muss die Möglichkeit bestehen, Meldung mündlich, schriftlich oder auf Wunsch persönlich abzugeben. Anonyme Meldungen sollen aber auch bearbeitet werden. Es besteht die freie Entscheidung, wo eine Meldung abzugeben ist, dabei sind interne Meldestellen zu bevorzugen.



v) Fristen

Eine Eingangsbestätigung muss innerhalb von 7 Tagen bestätigt werden und binnen 3 Monaten ist der Whistleblower über die ergriffenen Maßnahmen zu informieren. Es besteht Dokumentationspflicht.

vi) Repressalien; Beweislastumkehr

Repressalien gegen Whistleblower sind verboten, auch schon die Androhung und begründen einen Schadenersatzanspruch (§37 HinSchG). Der Gegenbeweis ist von der Organisation / dem Unternehmen zu erbringen (Beweislastumkehr §36 HinSchG).

(b) Hinweisgeber im Datenschutz (VVT)

Eine gute Vorlage ist die Orientierungshilfe zu Whistleblower-Hotlines der Datenschutzkonferenz der Aufsichtsbehörden (DSK) aus Ende 2018[4]. Zur Einordnung nach den Vorschriften zum Verzeichnis der Verarbeitungstätigkeiten (Erläuterung Fußnote[5]):

- ***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

3 *Quelle: Bundesregierung: „Besserer Rechtsschutz für „Whistleblower“*
4 *Quelle: DSK: „Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines“ (PDF)*
5 *Hinweis: V. Schroer: „Zusammenfassende Erläuterung zum Verzeichnis der Verarbeitungstätigkeiten“*

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/innen (§15 HinSchG).

- ***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:***

Rechtsgrundlage ist die Verpflichtung nach dem HinSchG (Art.6 Abs.1c DSGVO).
Lösch- bzw. Aufbewahrungspflicht: 2 Jahren nach dem HinSchG §11 Nr. (5).
Besonderheiten: Die Informationspflicht an einen Beschuldigten besteht nicht, wenn eine wirksame Untersuchung dadurch behindert wird. Die Besonderheiten für Empfänger, Transfer, Drittland u. ä. sind zu beachten.

- ***Schutzkonzept:***

Aufgrund des hohen Schadenspotentials für den Betroffenen sind zum bestehenden Schutzkonzept (TOM) umfangreiche Schutzmaßnahmen zur deutlichen Reduzierung der Eintrittswahrscheinlichkeit zu treffen (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[6], Zusammenfassung SDM, Seite 7).

3. Zur Datensicherheit

(a) Virenschutz

Dass ein Schutzprogramm / Virenscanner unverzichtbar ist, zeigen die aktuellen bis täglichen Warnung und die Vielzahl der wichtigen „Systemupdates“ zum Schutz vor bekannten Schadprogrammen.

i) Gratis oder kostenpflichtig

Wie immer, ist es eine Frage der Anforderungen. Wie aktuelle Testbewertungen zeigen, kann eine Gratis - Version für einen Einzelplatzrechner oder Mobilgerät ausreichend sein. Ein Blick auf die Auswertungen des unabhängigen, Magdeburger AV - Test Instituts[7] kann bei der Entscheidung hilfreich sein. Geht es an Mehrplatzrechner oder Client – Server – Strukturen mit Fernzugriff, vielleicht noch über Drittgeräte, sollte ein Spezialist mit entsprechendem Support hinzugezogen werden. Hilfestellung zum Einstieg gibt es auch vom BSI unter: „Wie Sie Ihren Computer sicher einrichten“.

ii) Online - Virenscanner

Es erscheint zunächst leichter, da keine Installation erforderlich und immer die aktuellste Prüfroutine genutzt wird. Allerdings fehlt der Wächter im Hintergrund, der jede aufgerufene Datei auf Signaturen prüft, er steht Offline nicht zur Verfügung, erfordert die Ausführung aktiver Inhalte (ActiveX) und muss möglicherweise über eine infizierte Onlineverbindung genutzt werden. Nützlich kann ein Onlinescanner helfen, wenn auf einem ungeschützten Rechner eine Infizierung vermutet wird oder für Einzelprüfungen, wie bei VirusTotal (Zusammenschluss von 70 Anbietern)[8].

iii) Empfehlung(en)?

Ein Virenscanner muss tief in die Systemarchitektur eingreifen können und sollte langfristig eingesetzt werden. Deshalb sind strenge Kriterien anzulegen und neben der Software sollte auch der Anbieter kritisch unter die Lupe genommen werden.

4. Zu angrenzenden Themen

Bei Bedarf, einfach mal sprechen!

6 *Hinweis: V. Schroer: „Zusammenfassung Das Standard - Datenschutz - Modell | Management – Info“*
7 *Quelle: AV Test GmbH: „Testübersichten“, für „Privatanwender“, für „Unternehmen“*
8 *LINK: VIRUSTOTAL*