Juli 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) EU – US – Data – Privacy - Framework: Fluch oder Segen?

Von heller Begeisterung (*Bitkom: „Dreijährige Hängepartie geht zu Ende“*)[1] bis erneute Klage vor dem EuGH (*noyb/Schrems: „Kopie des gescheiterten „Privacy - Shields“*)[2] reichen die Reaktionen auf den dritten Anlauf.

1 Quelle: tagesschau.de: „EU und USA Neues Datenschutzabkommen in Kraft“
2 Quelle: noyb.eu: „Europäische Kommission gibt EU-US Datentransfers 3. Runde beim EuGH“

i) Warum die Aufregung?

Für einen Datentransfer in ein Drittland (zur EU) gilt der Grundsatz: „Der Datenschutz reist mit den Daten!“ (*Kurze Checkliste habe ich hier als PDF verlinkt*). Die einfachste Prüfung ist die Vorlage eines EU - Angemessenheitsbeschlusses, d. h. die EU hat die Angemessenheit des Datenschutzes nach DS-GVO geprüft. Für US-Unternehmen braucht es nur noch eine Zertifizierung nach dem Trans – Atlantic – Data – Privacy - Framework und der Datentransfer ist mit dem Datenschutz nach DS-GVO vereinbar.

ii) Wo ist das Problem?

Noyob schreibt dazu u. a., dass der EuGH bereits feststellte, dass die Massenüberwachung (von Nicht-US-Bürgern) nach dem „*Foreign Intelligence Surveillance Act (FISA), Section 702*“ nicht verhältnismäßig ist, der Rechtsbehelf über den Ombudsmann würde nicht im Entferntesten dem *Artikel 47 der EU - Grundrechtecharta* entsprechen und im Übrigen wäre das neue Abkommen eine Kopie von 2016. Internet World schreibt dazu: „*Das EU-US-Datenschutzabkommen ist völlig wertlos, ein Fiasko für die Wirtschaft*“[3].

iii) Und jetzt?

Positiv zu vermerken bleibt die Reaktion des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit[4]:

> *„Mit dem neuen Angemessenheitsbeschluss können ab sofort personenbezogene Daten aus der EU an die USA wieder fließen, ohne dass weitere Übermittlungsinstrumente oder zusätzliche Maßnahmen erforderlich sind. Dies gilt jedoch nur, sofern die Organisation, an die sie übermittelt werden, auch unter dem EU - U.S. Data – Privacy - Framework zertifiziert ist.“*

Nach den jetzt gültigen Regelungen kann mit einem zertifizierten US-Unternehmen ein Datentransfer vorgenommen werden. Allerdings können die letzten Zweifel erst ausgeräumt werden, wenn der EuGH dazu angerufen wurde und sein Urteil verkündet. Es bleibt also in den nächsten Jahren zu beobachten und Zeit, um einen Notfallplan B für den Fall der Fälle ins Auge zu fassen, oder gleich eine der sicheren Alternativen zu wählen.

3. Zur Datensicherheit

(a) Basiselemente der Cyber-Sicherheit Nr. 5 „Makros“

Makros können ein Segen sein, um sich wiederholende, regelmäßige Vorgänge mit einem Klick (Makro) auszuführen. Leider können solche Makros auch ein Fluch sein, denn es lassen sich auch ganze Programme darin „verstecken“. Wie dem ESET Threat Report H1 2023[5] zu entnehmen, gehörten Office-Makros über viele Jahre zu den größten Cyberbedrohungen global. Mittlerweile hat Microsoft in den Standardeinstellungen Makros deaktiviert. Neben den selbst erstellen Makros besteht die Gefahr, schädliche Makros von Dritten über E-Mail und Dateianhängen, Download, Erweiterungen (Addons), Programminstallationen u. ä. zu erhalten. Makros können auch in anderen Dateien (z.B. PDF) versteckt sein. Wie immer ist die Konfiguration ein Kompromiss aus Sicherheit versus Komfort und Funktionalität.

i) Sicherheitseinstellungen einordnen

Sehr hoch	Nur Makros aus vertrauenswürdigen Dateiquellen werden ausgeführt. Alle anderen Makros werden deaktiviert, unabhängig von einer Signatur.
Hoch	Nur signierte Makros aus vertrauenswürdigen Quellen werden ausgeführt. Nicht signierte Makros werden deaktiviert.
Mittel	Bestätigung vor dem Ausführen von Makros aus nicht vertrauenswürdigen Quellen.
Niedrig	Alle Makros ausführen ist nicht empfehlenswert, nur wenn sichergestellt ist, dass nur sichere Dokumente geöffnet werden können.

3 Quelle: Internet World: „Das EU-US-Datenschutzabkommen ist völlig wertlos, ein Fiasko für die Wirtschaft“
4 Quelle: BfDI Pressemitteilung: „Angemessenheitsbeschluss zum EU-U.S. Data Privacy Framework in Kraft getreten“
5 Quelle: eset: „Threat Report H1 2023 December 2022 – May 2023 (PDF)"

ii) Und jetzt?

Gute und vertrauenswürdige Programmanbieter haben die Ausführung von Makros bereits in den Voreinstellungen deaktiviert und geben einen Warnhinweis vor Aktivierung aus. Ein Blick in Office und Kommunikationsanwendungen ist sicher hilfreich und beruhigend (meist unter „Trust Center, Sicherheit und Datenschutz u. ä.).

Für mittelgroße und große Organisationen, die Endsysteme mit Gruppenrichtlinien in einer Active – Directory - Umgebung verwalten, gibt die BSI Empfehlungen mit Schwerpunkt auf Microsoft Office Anwendungen[6]. Die zur Weitergabe an den IT – Service (bzw. Dienstleister) sehr zu empfehlen sind.

4. Zu angrenzenden Themen

(a) EU – DATA - ACT, was ist das denn jetzt?

Es geht um „freie Daten für den Wirtschaftsaufschwung“[7], mit Schwerpunkt auf die breite Nutzung von Daten vernetzter Geräte, wie Sprachboxen, Smartwatches, E-Autos, Smart-Home-Systemen bis hin zu industriellen, wie landwirtschaftlich genutzten Geräten und Robotern. Es besteht die Pflicht, Gerätedaten (ohne Personenbezug) von technischen Geräten zur Verfügung zu stellen.

i) Die guten Nachrichten:

- ✔ Wie bei der DS-GVO sind Kleinunternehmen (weniger als 50 Personen, weniger als € 10 Mio. Umsatz) ausgenommen.
- ✔ Verbraucher wie Unternehmen können von Dateninhabern neben den personenbezogenen Daten nach Art.20 DS-GVO auch die Herausgabe der nicht personenbezogenen Gerätedaten verlangen (Art.5 EU-Data-Act) und in Eigenverantwortung auch weitergeben.
- ✔ Das EU-Gesetz zielt auch darauf ab, die Dominanz der US-amerikanischen Technologiegiganten einzudämmen: Große Cloud-Anbieter wie Amazon Web Services, Microsoft und Google werden demnach dazu verpflichtet, illegalen Zugriff auf Daten zu verhindern und Standards für einen erleichterten Anbieterwechsel zu etablieren.

ii) Konflikte:

- ✗ Es besteht sogar die Pflicht des Dateninhabers seine Daten mit Dritten zu teilen, also Schnittstellen zum leichteren Austausch zu schaffen. ABER, diese Daten dürfen keine Rückschlüsse auf Personen zulassen (DS-GVO), sind also zu anonymisieren, ein Pseudonymisierung (Personenbezug in separater Speicherung) ist nicht erlaubt.
- ✗ Es besteht die Befürchtung, Geschäftsgeheimnisse könnten durch die Pflicht zur Datenweitergabe in Gefahr geraten. Die Offenlegung von Daten zu Geschäftsgeheimnissen besteht ausdrücklich nicht. Für Streitigkeiten soll eine zugelassene Stelle zur Beilegung von Streitigkeiten angerufen werden (Art.10 EU-Data-Act).
- ✗ Es bleibt wenig Zeit, da der Data - Act nach 20 Monaten inkrafttreten soll.

Ohne tief in die Thematik eingestiegen zu sein, würde ich sagen: „Da ist noch viel Musik drin, für die Unternehmen, die es anwenden müssen“.

Bei Bedarf, einfach mal sprechen!

6 *Quelle: BSI: „Empfehlungen: IT in Unternehmen, Sichere Konfiguration von MS Office…“*
7 *Quelle: tagesschau.de: „EU-“Data Act“ neue Regeln zur Daten-Weitergabe von Geräten“*
Quelle. EUR-Lex: „DOK 52022PC0068 EU-Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz)“