Oktober 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

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) „Drittlandtransfer, ungelöst, wieder in aller Öffentlichkeit! - Kurz mal durchgelüftet“

Wie war das nochmal?

i) Schrems II Urteil

Über Datenschutzkreise hinaus sehr gut bekannt ist das (sogenannte) Schrems II Urteil des EuGH vom 16. Juli 2020 (C-311/18)[3]. Zu den Auswirkungen hat der Bundesbeauftragte (BfDI)[4] in einer 3-

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: Info Curia: „EuGH Aktenzeichen = C-311/18“*
4 *Quelle: BfDI: Schrems II Urteil des EuGH (Urteil v. 16. Juli 2020, C-311/18) – Kernaussagen.“*

seitigen Stellungnahme Position bezogen und dazu ein „Prüfschema Drittstaatentransfers“ veröffentlicht[5].

ii) US-Datenrecht

Übrigens, die wissenschaftlichen Dienste des Deutschen Bundestages haben auf Anfrage aus dem Bundestag eine Stellungnahme / Dokumentation zum US-Datenrecht aus deutscher Datenschutzsicht erstellt[6]. Sehr interessante und übersichtliche Ausführungen zum Thema.

iii) Aufsicht weitet Prüfung aus

Das Handelsblatt berichtete unter dem 13. April 2021[7] von Ausweitungen der Prüfung durch Aufsichtsbehörden, u. a. zur US – Cloud - Nutzung.

iv) Was ist mit Großbritannien?

Wie haufe-online im August 2021 berichtete[8], gibt es für Großbritannien einen Angemessenheitsbeschluss der EU, der aber nach 4 Jahren überprüft werden muss. Wenn die Briten allerdings, wie vorgesehen, sich durch eine Reformierung von der DS-GVO trennen wollen, kann dieser auch früher hinfällig werden und Großbritannien gilt dann als Drittland, was im Auge zu behalten ist.

v) Die laufende Abmahnwelle

Dann war und ist da noch die aktuelle Welle der Abmahnungen wegen Einbindung von „google-fonts“ in die eigene Website. Eine Vielzahl der Kommentierungen sieht eine Unrechtmäßigkeit wegen notwendiger Übermittlung der IP-Adresse darin, man sollte aber nicht zahlen (i.d.R. zwischen 100€ bis 200€). Jedoch sind die „google-fonts“ sofort lokal einzubinden, oder gleich eigene Schriftarten einbinden (z.B. siehe Fußnote[9]).

vi) Neues US-Dekret zum Datenschutz

Aktuell – unter vielen anderen – berichtet die tageschau am 7. Oktober 2022 zum Vorstoß des US-Präsidenten mit einem neuen Dekret zum Datenschutzabkommen[10].

vii) Vorsichtiges Fazit:

Bis der Beschluss zum Dekret und ein mögliches, neues Privacy Shield besteht, wird es noch Monate dauern. Ob das Privacy Shield dann vor dem EuGH Bestand hat, muss sich erst noch zeigen. Max Schrems steht bereits in den Startlöchern und sieht einen Verstoß gegen die EU Grundrechtecharta. Es sieht eher nach eine Verschnaufpause als nach einer Lösung aus. Zwei Hinweise noch:

- Fernzugriff aus einem Drittland (z. B. Support) und / oder Speicherung in einer Cloud außerhalb der EU ist immer als Übermittlung anzusehen (Europan Data Protection Supervisor).
- Auch nur bei der Durchleitung über ein Land mit nicht angemessenem Schutzniveau, ist die Einhaltung der Sicherheit von personenbezogenen Daten zu gewährleisten.

(b) Info & kurze Checkliste zu Drittlandtransfer (10/2022)

[LINK] … einschließlich Erläuterungen zu ggf. erforderlichen, „zusätzlichen Maßnahmen“ des European Data Protection Board (edpb).

3. Zu Datensicherheit

(a) Cyberangriffe können jeden treffen

Ob Studien vom IT-Branchenverband Bitkom[11], PWC, dem jährlichen Lagebericht des Bundesamtes für Informationssicherheit[12] (den hat übrigens schon der Vize Dr. Schabhüser gezeichnet), oder einfach nur der allgemeinen Presse ist zu entnehmen, die Sicherheitslage in Deutschland ist angespannt bis kritisch. Durch die Verfeinerung der kriminellen Wertschöpfungs-

5 *Quelle: BfDI: „Prüfschema Drittstaatentransfers“*
6 *LINK: Wissenschaftliche Dienste des deutschen Bundestages: „US-Datenrecht, Zugriff von US – Behörden“*
7 *Quelle: Handelsblatt: „Deutsche Firmen in der Datenschutzfall – Behörden intensivieren Ermittlungen“*
8 *Quelle: haufe-online: „Großbritannien will Datenschutz reformieren und sich von der DSGVO lösen“*
9 *LINK: anwalt.de: „Abmahnungen wegen Google Fonts“*
10 *Quelle: tagesschau: „Vorstoß für ein neue Datenschutzabkommen (Vereinbarung mit der EU)“*
11 *Quelle: CSO Deutschland: „Bitkom-Studie: 203 Mrd. Euro Schaden pro Jahr in Deutschland“*
12 *Quelle. BSI: „IT-Sicherheitslage spitzt sich zu, die Lage der IT-Sicherheit in Deutschland 2022“*

ketten (117 Millionen neue Schadprogramme in diesem Jahr) kann es heute so gut wie jeden Treffen. Beflügelt werden die Angriffe durch die starke Zunahme des Homeoffice, möglichst noch mit privaten Geräten (BYOD), aber auch durch teilweise noch im Einsatz befindliche, alte Systeme in der Industrie.

(b) Noch mal Homeoffice

Auch für den Heimarbeitsplatz sind Verhaltensregeln, wie organisatorische Anweisungen und technische Schutzmaßnahmen zu beachten, die in einer Richtlinie festgehalten werden sollten und ggf. mit einem Betriebsrat abzustimmen sind. Ein erstes Muster finden Sie hier [LINK] und sollte individuell angepasst werden. Die wichtigsten Punkte:

- ✔ Keine Kenntnisnahme Dritter von Gesprächen, Unterlagen, Zugriffsberechtigungen u. ä. Ein abschließbares Arbeitszimmer, mindestens verschließbare Schränke wären hilfreich.
- ✔ Möglichst ein, vom Arbeitgeber sicher konfigurierte Rechner, bzw. die Einhaltung entsprechender Sicherheitsstandards (aktueller Virenschutz, Firewall, Verschlüsselungssoftware u. ä.), was zu überprüfen wäre. Datenspeicherung nur auf Firmennetzwerk oder -datenträgern.
- ✔ Eindeutige Trennung von beruflicher und privater Verarbeitung, möglichst über getrennte Endgeräte oder einer softwarebasierten (z. B. Container-) Lösung. Keine Weiterleitung von beruflichen E-Mails an privat Mailadressen.
- ✔ Bei LAN/WLAN dürfte es hpts. über den privaten Router gehen. Neben einer sicheren Passwortverschlüsselung bieten sich getrennte Netze und ein MAC-Filter an. Zusätzlich sollte das Firmennetzwerk nur über eine zusätzlich gesicherte VPN-Verbindung erreichbar sein.
- ✔ Die Datenschutzregeln sind entsprechend auch zu Hause einzuhalten!
- ✔ Sicher sind Ihre Mitarbeiter auch in Datensicherheit und Datenschutz geschult und bei Unsicherheit oder Datenpannen steht das Unternehmen hilfreich zur Seite. Schützen Sie Ihrer Mitarbeiter, aber vermeiden Sie übergriffige Kontrollmaßnahmen.

4. Zu angrenzenden Themen

(a) Informationsflut stresst Mitarbeiter

IT-Business berichtet[13], dass Deutsche Arbeitnehmer gestresst und überlastet sind. Dazu führen einer Operntext-Umfrage zufolge verschiedene Faktoren, wie der konstante Fluss von Daten über verschiedene Geräte hinweg, die allgegenwärtigen sozialen Medien oder die zunehmende Anzahl von Anwendungen, denen Arbeitnehmer im Arbeitsalltag ausgesetzt sind. Wegen genau dieser Informationsflut fühlen sich 82 Prozent der Deutschen gestresst.

(b) Gefährliche Zwangs-Apps für Fußballfans

Die Fußball-WM in Katar ist ohnehin problematisch. Nun müssen sich Fußball-Fans darauf gefasst machen, mit Handy-Apps überwacht zu werden so Netzpolitik.org[14].

Sorgen bereitet einerseits die App: „Ehteraz“, die Infektionen mit dem Coronavirus nachverfolgen soll. Einmal installiert, kann sie u. a. auf sämtliche Daten auf dem Handy zugreifen, WLAN- oder Bluetooth-Verbindungen überwachen, den genauen Standort auslesen und speichert auf einer zentralen Datenbank. Die andere App: „Hayya“, ist die offizielle App für die Weltmeisterschaft zur Verwaltung der Veranstaltungen. Weniger invasiv, greift aber dafür kritische Daten ab und kann u.a. den Standort auslesen, das Smartphone am Einschlafen hindern und Netzwerkverbindungen überwachen. Ferner sei sie in der Lage, persönliche Informationen „beinahe ohne Einschränkungen“ weiterzugeben.

Einige erinnern sich vielleicht noch dazu an den Einsatz der Spionage-Software „Pegasus“[15] der Geheimdienste. Besser ein billiges „Einmal-Smartphone“ mitnehmen, sicher ist sicher!

Bei Bedarf, einfach mal sprechen!

13 *Quelle: IT-Business: „Informationsflut stresst Arbeitnehmer“*
14 *Quelle: Netzpolitik.org: „WM in Katar, gefährliche Zwangs-Apps für Fußballfans“*
15 *Quelle: deutschlandfunk.de: „Spionage-Software Pegasus“*