Juli 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.....1

Letzte Ergänzung: 11/2021: Baustein 51 (zu TOM).....1

2. Zum Datenschutz.....1

(a) Stärkung der Verbraucherrechte.....1

i) „Der Kündigungsbutton“.....1

ii) Klagen von Verbraucherverbänden rechtens.....2

iii) „Die UPDATE – Pflicht“.....2

(b) Anbieter von Videokonferenzen nicht mehr Auftragsverarbeiter.....2

3. Zur (IT-) Datensicherheit.....2

(a) Jeder 2te Angestellte umgeht Sicherheitslösungen....2

(b) Risiko zu IIoT und OT hoch.3

4. Zu angrenzenden Themen.....3

(a) Systemschutz schon mit wenigen Mitteln.....3

(b) Gravierende Sicherheitsmängel in mehreren Kita-Apps.....3

(c) Datenleck Twitter.....3

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) Stärkung der Verbraucherrechte

i) „Der Kündigungsbutton“

Wie auf der Seite des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) veröffentlicht[3], kommt der Kündigungsbutton bzw. muss kommen!

(BGB § 320k) Gesetz ist seit 01.07.2022, dass bei abgeschlossenen, zu bezahlenden Dauerabonnements, ob Handy, Streaming, Zeitungen, Fitness usw., unabhängig vom Abschlussdatum und der Ursprungsform, auf der Website eine Kündigungsbutton in gleich – guter Sichtbarkeit wie

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: BMUV: „Verbraucherrechte online werden gestärkt“*

der Abschlussbutton vorhanden sein muss. Die Kündigung sollte mit zwei Klicks abgeschlossen und vom Unternehmen umgehend bestätigt werden. Ohne Datumsangabe gilt der früheste Kündigungstermin.

ii) Klagen von Verbraucherverbänden rechtens

In einem Verfahren zur Klage der Verbraucherzentrale Bundesverband gegen Meta/Facebook hatte der BGH wegen Zweifel an der Gültigkeit der Klage, korrekterweise den EuGH um Entscheidung gebeten. Mit Urteil C-319/20[4] vom 28.04.2022 hält der EuGH fest, dass die Klage eines Verbandes ohne Auftrag und ohne konkrete Verletzung:

> *„nichts entgegensteht, sofern die betreffende Datenverarbeitung die Rechte identifizierter oder identifizierbarer natürlicher Personen aus dieser Verordnung beeinträchtigen kann“.*

Die Frage der TRANSPARENZ gegenüber dem Verbraucher, insbesondere die Einwilligung, dürfte für Verbraucherschützer im Fokus stehen. Ist der Verbraucher verständlich und vollumfänglich über die erhobenen Daten, den Zweck und die Verarbeitung informiert und hat genau dazu seine Einwilligung gegeben?

iii) „Die UPDATE – Pflicht“

Bereits zum 01.01.2022 ist der BGB § 327f Aktualisierungen in Kraft. Darin lautet es in Absatz (1):

> *„Der Unternehmer hat sicherzustellen, dass dem Verbraucher während des maßgeblichen Zeitraums Aktualisierungen, die für den Erhalt der Vertragsmäßigkeit des digitalen Produkts erforderlich sind, bereitgestellt werden und der Verbraucher über diese Aktualisierungen informiert wird. Zu den erforderlichen Aktualisierungen gehören auch Sicherheitsaktualisierungen.“*

Ziel sind vor allem Anbieter von IoT / Smart - Home Geräten, da nach Bericht der IoT – Security – Foundation aus November 2021[5] hier die Lage völlig inakzeptabel ist. 80 % aller Vertriebsfirmen von IoT – Geräten reagieren gar nicht oder nur unzureichend auf gemeldete Sicherheitslücken, zumal diese es nicht schaffen, einfachste Maßnahmen wie ein Meldesystem zu implementieren. Dabei wurde die Strategie in Form der Konzeption und Regelwerke analysiert und noch nicht einmal die Geräte selbst. Eine „Ampel – Liste“ zur Einordnung der Hersteller befindet sich auf Seite 20ff des Berichts.

(b) Anbieter von Videokonferenzen nicht mehr Auftragsverarbeiter

Laut 27. Datenschutzbericht 2022 der Landesbeauftragten für Datenschutz und die Informationsfreiheit NRW[6] (DS-GVO konform: JA, aber kein Auftragsverarbeitungsvertrag mehr notwendig):

> *„Auch Videokonferenzdienste, die bis zum 1. Dezember 2021 als Telemediendienste eingeordnet wurden, sind nunmehr als Telekommunikationsdienste zu bewerten. Das führt unter anderem dazu, dass Stellen, die Videokonferenzdienste einsetzen, keinen Auftragsverarbeitungsvertrag mehr mit den Videokonferenzanbieter*innen abschließen müssen und für die aufgrund der Übertragung des Videochats verarbeiteten personenbezogenen Daten nicht mehr verantwortlich sind. Selbstverständlich sind sie nach wie vor dazu verpflichtet, technische und organisatorische Maßnahmen zu treffen, wie zum Beispiel datenschutzfreundliche Grundeinstellungen vorzunehmen.“*

Das bedeutet aber auch, dass zum Setzen von Cookies grundsätzlich eine Einwilligung erforderlich ist (kein berechtigtes Interesse des Verantwortlichen). Ausnahme nach TTDSG § 25 gilt ausschließlich für zwingend notwendige Informationen zur Kommunikation (Sprache, Browser usw.).

3. Zur (IT-) Datensicherheit

(a) Jeder 2te Angestellte umgeht Sicherheitslösungen

Die Zeitschrift für Informationssicherheit <kess>[7] berichtet von einer CISCO – Studie über die Befragung von 1.000 Angestellten. Ca. 50 % der Befragten empfinden die IT – Sicherheitslösungen zu kompliziert, umständlich und zeitraubend, mit im Durchschnitt 15 Minuten täglichem Aufwand.

4 Quelle: EuGH C-319/20 vom 28.04.2022 auf InfoCuria
5 Quelle: IoT Security Foundation. „The contemporary use of vulnerability disclosure in IoT Report 4.11.2021“
6 Quelle: https://www.ldi.nrw.de/system/files/media/document/file/27_datenschutzbericht_2022_ldi_nrw.pdf
7 Quelle: <kess> „Jeder zweite Angestellte umgeht Security-Lösungen“

Um ihre Arbeit schneller zu erledigen, umgehen 55 % wöchentlich und sogar 17 % täglich die Sicherheitsmaßnahmen (*„gut gemeint oder das Gegenteil von gut“*).

Neben Information und Sensibilisierung der Mitarbeiter sollten die Sicherheitsmaßnahmen möglichst intuitiv nutzbar sein. Mittlerweile verbreitet ist die 2-Faktor-Authentifizierung über Authenticator Apps, z. B. von Sophos, Google, Microsoft, oder PhotoTAN / SMS von Banken und Online-Portalen, oder USB – Schlüssel – Keys (Infolinks – Beispiele in der Fußleister[8]).

Auf der anderen Seite zeigt die Studie, dass 38 % der Befragten ihrem Unternehmen in Bezug auf Sicherheit misstrauen. Deshalb fühlen sich 71 % mit Passwörtern wohl, 61 % noch mit Fingerabdruck und beim Gesicht – Scan nur noch 46 %. Transparenz ist da ein wichtiger Faktor.

(b) Risiko zu IIoT und OT hoch

So ein Bericht der Barracuda Network Inc.[9] zu *Industrial – Internet – of – Things* und Operational – Technology *(Marktforscherstudie mit 800 teilnehmenden Managern, Projektleitern, IT-Admins aus diversen Branchen)*.

- Mehr oder weniger als 90 % hatten in den letzten 12 Monaten einen Sicherheitsvorfall, sind ziemlich besorgt über die aktuelle Bedrohungslage und hatten mehr als einen Tag mit einer Sicherheitsverletzung zu kämpfen.
- Im verarbeitenden Gewerbe liegt die Implementierung von Sicherheitsprojekten bei lediglich 24 % und im Gesundheitsweisen bei nur 17 %. Mit Implementierung eines Sicherheitsprojektes haben 74 % davon keinerlei Auswirkung eines Vorfalls verspürt.
- Sicherheitsfokus sollte auf Konnektivität & Endgeräte, Netzwerksegmentierung, Netzwerk- & Webanwendungsfirewalls und Multi – Faktor – Authentifizierung liegen.

4. Zu angrenzenden Themen

(a) Systemschutz schon mit wenigen Mitteln

Liest man das „Register aktueller Cyber-Gefährdungen und – Angriffsformen v2.0“ (BSI / Cyber Alliance)[10], sind es nicht die Vielzahl der Begriffe (Whaling, Maskerade, Nicknapping, Replay usw.) die etwas erschrecken, sondern die Arten der Abläufe (siehe Definitionen; „Was es alles so gibt!“).

Die SOPHOS Ltd. © (internationale Sicherheitssoftware & -support / GB) gibt in einem Whitepaper 7 einfache Tipps um die eigenen Systeme zu schützen[11].

- ✔ Multi – Faktor – Authentifizierung (MFA) zwingend für Systemadmins und Sicherheitskonsolen
- ✔ Für externe Verbindungen zwingend das Remote – Desktop – Protcol (RDP) blockieren
- ✔ Alle Endgeräte sollten geschützt sein, auch wenn sie nur Offline sind
- ✔ Vermeidung von Hacker – Zugängen durch Schulung zu Phishing (Mail, Web) oder Identitäts-diebstahl durch strenge Berechtigungs- und Passwortkonzepte (mit mind. 2-Faktor-Auth.)
- ✔ Werkzeuge / Tools für Administration streng und eng begrenzen (Skalpell statt Hammer)
- ✔ Update, Update, Update, insbesondere externe Schnittstellen
- ✔ Erstellen Sie einen Vorfallplan (Incedent Responce Plan) für den Notfall

Über den Link in der Fußleiste kann das Whitepaper mit Erläuterungen angefordert werden.

(b) Gravierende Sicherheitsmängel in mehreren Kita-Apps

… entdeckt, so ein Bericht des Spiegels[12]. Nur 12 von 42 geprüften Apps mit denen Eltern und Erzieher kommunizieren sind unbedenklich (Verschlüsselung, Cloud-Speicher, Adressen u. ä.).

(c) Datenleck Twitter

Lt. „golem.de“ will ein Hacker 5,4 Mio. Datensätze von Twitter – Usern verkaufen.[13]

Bei Bedarf, einfach mal sprechen!

8 *LINKS Schlüssel-Keys: „yubico.com“, „Neowave Winkeo FIDO U2F“*
9 *Quelle: Barracuda Networks Inc.: „The state of industrial security in 2022.“*
10 *Quelle: BSI/Cyber Alliance: „Register aktueller Cyber-Gefährdungen und -Angriffsformen v2.0.“*
11 *Quelle: Sophos: „Erhöhen Sie jetzt Ihre Cybersicherheit! 7 Tipps, wie Sie Ihr Unternehmen gegen Cyberangriffe schützen “*
12 *Quelle: Spiegel: „Gravierende Sicherheitsmängel in mehreren Kita-Apps entdeckt.“*
13 *Quelle: golem.de: „Hacker will 5,4 Millionen Twitter-Datensätze verkaufen.“*