August 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) Verein: Mitgliederlisten & Datenschutz

Wer darf Mitgliederlisten mit Kontaktdaten einsehen und erhalten? Wird da nicht oft der Datenschutz vorgeschoben, weil man es nicht will? Aus einem Urteil des OLG Hamm 8 U 94/22 vom 26.04.2023[1]. Gestützt auf Art.6 Abs.1b) DS-GVO (erforderliche Verarbeitung aus Vertrag) darf:

- ✔ Der Vorstand zur Information der Mitglieder über vielfältige Themenbereiche, insbesondere für eine korrekte Einladung zur Mitgliederversammlung, Trainer / Gruppenleiter für ihre

1 *Quelle: Oberlandesgericht Hamm, 8 U 94/22: „Vereinsmitglied, Mitgliederliste, E-Mail-Adressen, Datenschutz“*

jeweilige Untergruppe. Alle Zugriffe im Sinne der rechtmäßigen Ausübung von Vereinsleistungen und Veranstaltungen.

Den Mitgliedern zur Kontaktaufnahme mit anderen Mitgliedern?

- ✔ JA, aus der besonderen (Vereins-) Beziehung der Mitglieder untereinander
- ✔ WENN keine anderen, überwiegenden Interessen dagegen stehen.
- ✔ NICHT mit einer werblichen Ansprache im Sinne des UWG verbunden ist.

„DS-GVO Art.6 Abs.1 f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.“

Dabei ist durch die Verantwortlichen ***immer einer Interessenabwägung*** durchzuführen. Wirksame Widersprüche einzelner Mitglieder müssen individuell begründet sein (z.B. Feindschaft mit, oder Stalking durch ein anderes Mitglied) und dargelegt werden.

(b) Dateneigentum (?!)

Mit dem EU – DATA - ACT (freie Daten für den Wirtschaftsaufschwung) „geistert“ gerade im Widerspruch die Idee vom Eigentum an Daten durch die Fachpresse. Detaillierte Auseinandersetzung mit dem Thema im CMS Deutschland Blog „Data Ownership – Keine Eigentumsrechte an Daten“[2].

Mit personenbezogenen Daten geht es mit der DS-GVO schon mal nicht. Es kann zwar ein Nutzungsrecht nach den Vorgaben der DS-GVO vereinbart werden („Einwilligung“ u.s.w.), allerdings muss dieses Nutzungsrecht auch jederzeit widerrufbar sein und bleiben.

Übrig bleiben also die „unpersönlichen Maschinendaten“. So kommt auch eine Arbeitsgruppe des Bundesministeriums für Wirtschaft und Energie zu der Erkenntnis:

„Eine generalisierte Zuweisung von Ausschließlichkeitsrechten an Daten, ohne zugleich diese Rechtsposition wieder relativierende Zugangs- und Teilhaberechte zu regeln, birgt ein hohes Risiko, vor allem innovationshemmend zu wirken und den gewünschten „Free Flow of Data“ erst gar nicht entstehen zu lassen.“ [3]

Mit anderen Worten, folgt man dem Gedanken des EU – Data – Acts, dann erfordern neue Technologien eine offene Gesellschaft und Informationen sind für die Informationsgesellschaft zu wichtig, um sie einer Eigentumsposition mit Exklusivrechten zuzuordnen.

3. Zur Datensicherheit

(a) Basiselemente der Cyber-Sicherheit Nr. 6 Schulen & Sensibilisieren

Ein wichtiger Sicherheitsfaktor zur Abwehr von Cyberangriffen ist der Mensch *(und nicht das Problem, um es mal deutlich zu sagen, denn nur Mensch kann noch verhindern, was die IT-Sicherheit nicht kann.)*. Damit er diese Anforderung meistern kann, sollte der Mensch regelmäßig sensibilisiert und geschult werden.

i) Information & Unterstützung durch:

- ✔ Verständliche Information über die technischen Sicherheitsvorkehrungen, deren Schutzwirkung und vor allem über deren Grenzen!
- ✔ Vermittlung eines guten Gefühls bei verdächtigen Aktivitäten (z. B. E-Mail) lieber eine Anfrage zu viel den IT-Verantwortlichen vorzustellen, als genau die „EINE“ zu wenig.
- ✔ Einfache Tipps, wie z.B. den 3-Sekunden-Sicherheits-Check[4] des BSI zu E-Mails (1. Kenne ich den Absender? 2. Ist der Betreff sinnvoll? 3. Erwarte ich den Anhang?) PLUS: 4.) Fehler im Text und sichtbare Links weichen von echtem Link ab (z.B. *„google.com“* zu *„gooogle.com“*).
- ✔ Wenige Grundregeln in der E-Mail Kommunikation erhöhen nicht nur die Effizienz, sondern

2 *Quelle: Blog CMS Deutschland: „Data Ownerschip – Keine Eigentumsrechte an Daten“*
3 *Quelle: Smart-Data-Begleitforschung FZI Berlin: „Daten als Wirtschaftsgut“ (PDF)*
4 *Quelle: BSI „Spam-Phishing & Co. So erkennen Sie gefälschte und schadhafte E-Mails“*

auch die Sicherheit zur Erkennung korrekter E-Mails. Zum Beispiel die Vermeidung unnötiger „Empfänger in „cc & bcc“, ein kurzer Betreff beginnend mit dem Grund (INFO: AUFGABE: ANTWORT: EILT: ERLEDIGT:) „|“ Termin(e) „|“ mit Stichwort zum Thema und bei jeder E-Mail vom Absender im 1. Absatz eine kurze Zusammenfassung der Erwartung an den / die Empfänger zur Mail.

- ✔ ...

ii) Informationen zu Angriffsflächen

- ✔ Um eine möglichst realitätsnahe Nachricht zu erstellen, sammeln Betrüger Informationen in sozialen Netzwerken und auf Plattformen. Deshalb ist mit persönlichen und geschäftlichen Informationen dort sehr verantwortungsvoll umzugehen. Keine Veröffentlichung von vertraulichen Informationen in sozialen – Netzwerken und überhaupt in der Kommunikation mit Dritten über den Arbeitgeber, die Organisation und die Arbeit.
- ✔ Zugangsdaten, Passwörter oder Kontoinformation niemals per Mail, Telefon oder Konferenz-systemen weitergeben, da die Gefahr des Mitlesens oder Mithörens besteht.
- ✔ Betrüger nutzen auch gerne Fernwartungssoftware (Remote – Services), um sich auf den eigenen Rechner aufzuschalten und durch Ablenkung Schadsoftware aufspielen zu können. Der 3-Punkte-Check vor Einsatz von Fernwartungssoftware 1.) Ist der Anbieter bekannt? 2.) Besteht eine Vereinbarung mit dem Serviceanbieter? 3.) Ist die Rechtmäßigkeit einer Ankündigung auf unabhängigem Kommunikationsweg bestätigt?
- ✔ „Wie Hacker Ihre Psyche entschlüsseln … und wie Sie sich davor schützen können. Psychotricks und Phishing-Maschen“ ein DIN A3 Poster der Allianz-für-Cybersicherheit[5] zeigt kurz und übersichtlich die Tricks und Maschen der Kriminellen. Ein Aushang kann die Aufmerksamkeit hochhalten.
- ✔ …

iii) „Outdoor – Office“

Auch wenn hinlänglich beschrieben, geschrieben, gesagt und gezeigt, fällt mir beim Reisen doch immer wieder auf, dass ein Minimum an Grundregeln nicht beachtet wird.

- SPERREN: Geräte sollten zwar nie unbeaufsichtigt sein, aber sobald man es „aus der Hand“ legt ist die Sperre (Passwort oder biometrische Sperren u. ä.) auf Smartphone, Laptop umgehend zu aktivieren.
- NETZ: Öffentliche WLAN – Netze sind immer ein Risiko für und mit sensiblen Daten. „Wenn es denn sein muss, nie ohne VPN (Virtual Privat Network; verschlüsselte Verbindung zwischen zwei Beteiligten). Im Zweifel lieber auf das Mobilfunknetz setzen, z. B. über die einen WLAN - Hotspot vom Smartphone mit VPN. Anleitung zur Ersteinrichtung von chip.de[6]
- VERSCHLÜSSELN: Damit im „Fall der Fälle“ kein unerlaubter Zugriff auf Rechner oder Smartphone erfolgt, ist eine Verschlüsselung angebracht, die meistens schon „an Board“ ist, mit BitLocker bei Windows, FileVault bei Mac-OS. Die Smartphones, iPhones wie Android ab Version 10 sind standardmäßig verschlüsselt.
- DISKRETION: „Mithören“ und „Mitsehen“ lässt sich in öffentlichen Räumen auch für Dritte meist schlecht vermeiden. Deshalb keine Telefonate oder Videokonferenzen zu vertraulichen Themen und Nennung von Namen / Daten / Fakten. Hilfreich ist auch eine Blickschutzfolie zur Vermeidung neugieriger Blicke.
- NIE KIOSK-PCs: … an Flughäfen oder in Hotels, wie unbekannte Hardware Dritter für Dienste mit sensiblen Inhalten und Zugangsdaten nutzen (z. B. Online-Banking). PS: Öffentliche Ladestationen über USB statt Netzstecker sind beliebte Angriffspunkte für Hacker.

4. Zu angrenzenden Themen

Bei Bedarf, einfach mal sprechen!

5 *Quelle. Allianz-für-Cybersicherheit: „Awereness-Poster „Psychotricks und Phishing-Maschen“*

6 *Link: chip.de: „Anleitung für die Ersteinrichtung im Praxistipp > Android von chip.de.“*