Juni 2024 | 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 Grundlage 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

Standard-Datenschutz-Modell *übersichtlich zusammengefasst 11 Seiten*	**Standard-Datenschutz-Modell** Datenschutzkonferenz DSK 77 Seiten	**Datenschutz-Grundverordnung** auf dejure.org	**Bundesdaten-schutzgesetz** auf dejure.org

Das SDM [*der Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder (DSK)*] überführt die rechtlichen Anforderungen der DS-GVO über 7 Gewährleistungsziele in die technischen / 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. | Aktuell: SDM Version 3.0 (12/2022) | Letzter Baustein 11/2021: Nr. 51 „Zugriff auf Daten, Systeme und Prozesse regeln“

2. Zum Datenschutz

(a) „Datenschutzleitfaden für kleine Unternehmen der EDSA“[1]

Der ‚Europäische Datenschutzausschuss‘ (EDSA) hat für kleine Unternehmen einen Datenschutzleitfaden auf den Webseiten der EU veröffentlicht und beantwortet die Fragen:

„Sind Sie nicht sicher, wie Sie die DSGVO einhalten sollen?“
„Verarbeiten Sie personenbezogene Daten über Ihre Mitarbeiter, Verbraucher und Geschäftspartner?“
„Möchten Sie die Datenschutzrechte verstehen?“

Die Erläuterungen mit Beispielen zum (bekannten 😉) Datenschutz sind sehr verständlich (auf Deutsch) beschrieben. Interessant sind auch die Hinweise zur Reaktion auf eine Datenschutzverletzung und die ggf. erforderliche Meldung an die zuständige Aufsichtsbehörde. Unter „Germany“[2] findet man auch gleich den Link zu seiner (den) zuständigen Aufsichtsbehörde(n) mit dem

1 *Link: EDSA Datenschutzleitfaden für kleine Unternehmen https://www.edpb.europa.eu/sme-data-protection-guide/home_de*
2 *Link: Meldeformulare der Aufsichtsbehörden: https://www.edpb.europa.eu/notify-data-breach_de*

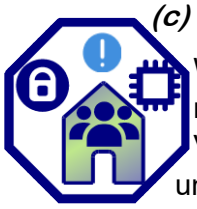
CC BY SA

Meldeformular zum direkten Ausfüllen und Abschicken. Gut zu wissen, besser ist natürlich, wenn es nicht gebraucht wird! 😉

(b) „Schadenersatz! Was für ein Schaden?“[3]

Der Europäische Gerichtshof hat wieder mal entschieden[4], auch wenn er nicht für eindeutige Klarheit gesorgt hat. Der EuGH wurde von verschiedenen deutschen Gerichten um Klarstellung zur Schadensbemessung befragt, u. a. auch zu immateriellen Schäden. Nach deutschem Recht (§§ 249 bis 253 BGB) ist ein erlittener Schaden (nachweisbar) Voraussetzung für einen Anspruch. Mit Art.82 DS-GVO kommen neben den materiellen Schäden auch immaterielle Schäden hinzu. Die Gerichte sind derzeit in einer Vielzahl von Verfahren mit der Festlegung der Höhe eines noch nicht eingetretenen, aber möglichen Schadens beschäftigt. Festzuhalten bleibt aktuell:

- ☑ Bei einem begründeten Anspruch kommt es lediglich darauf an, den entstandenen Schaden auszugleichen. Eine abschreckende Wirkung ist nicht Sinn und Zweck des Schadenersatzes nach DS-GVO. (Abschreckung übernehmen die Aufsichtsbehörden mit nicht unempfindlichen Bußgeldbescheiden).
- ☑ Allerdings kann (nach EuGH) schon die begründete Befürchtung, dass es zu einem Missbrauch der Daten kommen könnte, zu einem Schadenersatz führen. Die Bemessung der Höhe in diesen Fällen ist jedoch unklar geblieben. Deshalb sind viele Versuche vor Gericht gescheitert, bzw. die zugesprochenen Summen sind bei bisherigen Entscheidungen eher gering (2- bis 3-stelliger Bereich, siehe Link in der Fußnote)[5].



(c) Nachtrag zu „Haushaltsausnahme“

Wie im letzten Monat zur „Haushaltsausnahme“ beschreiben, sind die Grenzen dazu fließend, recht eng und in einigen bis vielen Fällen überschritten. Für eine darüber hinausgehende Verarbeitung (z.B. Bilder auf Social Media posten) wird in den wenigsten Fällen eine schriftliche und damit juristisch nachweisbare Einwilligung eingeholt worden sein. Das ist auch nicht zwingend erforderlich, in Art.4 Nr.11 DS-GVO lautet es:

> *"Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;*

Wenn es eine im Umfang „geübte, regelmäßige Praxis“ ist, den Betroffenen lange bekannt, ersichtlich und kein Widerspruch erfolgte, dürfte eine spätere Beschwerde / Schadenersatzforderung schwer geltend machen zu sein. Gleiches gilt für eine Einwilligung im Gespräch, oder die Preisgabe der Kontaktdaten zur Verarbeitung im Adressbuch des Smartphones, oder die Übergabe einer Visitenkarte u. ä.

(d) Umfang des Auskunftsrechts

Nach Art.15 DS-GVO hat die betroffene Person ein Recht auf Auskunft über die Verarbeitung seiner Daten. Der BGH hatte in einem Urteil aus Februar d. J[6]. über den Umfang zu entscheiden. Aus der Entscheidung kurz festgehalten:

- ☑ Das Auskunftsrecht nach der DS-GVO umfasst alle Dokumente, die von und für die betroffene Person erstellt wurden. **Aber**
- ☑ Telefon-, Gesprächsnotizen oder interne Vermerke sind nicht pauschal vom Auskunftsrecht erfasst! Nur wenn zur Nachvollziehbarkeit der Datenverarbeitung im Gesamtzusammenhang erforderlich, fallen diese Dokumente auch unter das Auskunftsrecht, damit der

3 *Quelle: Legal Tribune Online, 20.06.2024 EuGH zur DSGVO: Datenklau als immaterieller Schaden?*
4 *Quelle: InfoCuria: „EuGH-Urteil C-182/22 und C-189/22 Anspruch auf Ersatz des Schadens nach der DSGVO.“*
5 *Quelle: CMS law tax future: „DSGVO-Schadenersatz Übersicht, aktuelle Urteile und laufende Entwicklung“*
6 *Quelle: dejure.org: „Volltextveröffentlichungen BGH, 06.02.2024 – VI ZR 15/23“*

Betroffene seine Rechte *zur Verarbeitung* seiner Daten effektiv ausüben kann.

3. Zur Datensicherheit

(a) Warnung vor Cyberattacken über Office 365 Komponenten

Das Landeskriminalamt veröffentlichte unter diesem Titel folgende Warnung, da bereits mehrere Firmen vor Angriffen geschützt werden konnten:

Im Rahmen von aktuellen Ermittlungen durch das Landeskriminalamt Nordrhein-Westfalen wurde festgestellt, dass derzeit viele Unternehmen von Cyberangriffen auf Office 365 (E-Mail und Dokumentenverwaltung) betroffen sind. Diese Angriffe bergen Gefahren auch für angebundene Firmen des Unternehmensnetzwerks sowie für deren Kunden und Kommunikationspartner.

Unbekannte Täter übernehmen E-Mail-Konten und versenden dann Nachrichten im Namen der betroffenen Firmen. Diese E-Mails enthalten gefährliche Anhänge oder Links. Die E-Mails sehen echt aus, da sie keine Sprachfehler, dafür aber oft echte frühere Gesprächsverläufe enthalten. Sobald ein Empfänger auf die Links klickt, kann das IT-System unmittelbar angegriffen werden, und es kann zu Datenverlust bzw. dem Diebstahl von Daten sowie weiteren Angriffen zum Beispiel Phishing Attacken kommen.

Die Täter durchsuchen außerdem die übernommenen E-Mail-Konten gezielt nach Informationen aus der Anfangszeit der Corona-Krise, besonders nach VPN-Zugangsdaten nicht öffentlicher IT-Netzwerke. Diese Informationen ermöglichen es den Tätern, direkten Zugriff auf die IT-Infrastruktur von Unternehmen zu erhalten. Auch auf Dokumente in den E-Mails können sie zugreifen.

(b) Von „IT-“ zur „OT-“ Sicherheit?

Was für die Information Technology (IT) sollte auch für die Operation Technology (OT) gelten. Durch die zunehmende Vernetzung von produktiven Systemen mit der Datenverarbeitung (IT) und dem Internet in Zeiten von Industrie 4.0, bietet dieses auch Angriffsflächen für Hacker und ist zu schützen. Klingt einfach, ist es aber nicht, da die Software a.) abhängig vom Hersteller und b.) i.d.R. für die Produktionsmaschine speziell entwickelt wird. Einige Fragen zur Sicherheit sind:

- Wird die Sicherheit vom Hersteller laufend geprüft, werden bei Bedarf frühzeitig Updates ausgeliefert und sind Soft- und Hardwareschwachstellen in der Lieferkette auszuschließen?
- Sind Anschlüsse für Wechseldatenträger und mobile Systeme auf das Notwendigste begrenzt und gesichert?
- Sind Zugänge zum Internet und über Fernwartungszugänge gesichert und auf das Notwendigste beschränkt?

Das Bundesamt für Sicherheit in der Informationstechnik hat dazu Standards entwickelt (verlinkt):

- Zusammenfassende Managementinformation ISMS (6 Seiten)

und für weitere Informationen für Interessierte und Spezialisten direkt zum BSI:

- BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS, 48 Seiten)
- BSI-ICS-Security-Kompendium (speziell für die OT-Sicherheit, 122 Seiten)
- BSI-ICS-Security-Kompendium für Hersteller / Integratoren (Anforderung & Test, 44 Seiten)

4. Zu angrenzenden Themen

(a) Eigentlich immer die gleiche Masche

… nur anders, perfider, wie chip.de zu einer Warnung der Experten von Proofpoint berichtet.[7] Es werden echt aussehende Fehlermeldungen z. B. des Browsers, oder des Betriebssystems angezeigt mit Hinweis, zur Behebung einen Code (per COPY-Button) in PowerShell (Windows Terminal) zu kopieren und auszuführen (Enter). TIPP: NIE und NIMMER! 😡

Bei Bedarf, einfach mal sprechen!

7 Quelle: chip.de: „Versteckt in unscheinbaren Popups: Forscher warnen vor gefährlicher Sicherheitslücke“