Februar 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.....1

2. Zum Datenschutz.....1

(a) Falscher Empfänger personenbezogener Daten.....1

i) Für den Versender.....1

ii) Für den Empfänger.....2

3. Zur Datensicherheit.....2

(a) Doxing?.....2

i) Vorgehen.....3

ii) Schutz.....3

4. Zu angrenzenden Themen.....3

(a) Wie kommen die an meine Daten?.....3

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) Falscher Empfänger personenbezogener Daten

„Keiner ist perfekt“ (!), insbesondere in der digitalen Kommunikation, z. B. ist bei Mails schnell der falsche Adressat eingetragen und die Daten sind raus. Eine klassische Datenschutzverletzung. Wie damit umgehen?

i) Für den Versender

Nach Art.33 DS-GVO sind Datenschutzverletzung innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde zu melden, es sei denn, dies führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen. Besteht ein hohes Risiko, hat nach Art.34 DS-GVO der Verantwortliche die betroffene Person unverzüglich von der Verletzung zu informieren. Ein mögliches Vorgehen:

✔ Schaden begrenzen: Mit dem Empfänger umgehend in Kontakt treten und ihn bitten, die Mail / Daten sofort ungesehen / ungenutzt zu vernichten und dies zu bestätigen, sofern nicht selbstständig die Daten gelöscht, verschlüsselt oder anderweitig vernichtet oder vor Zugriffen

CC BY SA

geschützt werden können.

- Risiken einschätzen: Welche Risiken können aus dem Verlust der Daten entstehen, wie mögliche finanzielle Schäden, Identitätsdiebstahl, Ruf-/Imageschäden, Bloßstellung, Geheimnisoffenbarung, Existenzgefährdung oder sind es eher geringe bis keine Auswirkungen. Am besten die Einschätzung mit einem Datenschutzbeauftragten vornehmen, bzw. abstimmen. Für Interessierte hat die Datenschutzkonferenz des Bundes und der Länder ein „Kurzpapier" herausgegeben.[1]
- Betroffene informieren: Nach meiner Einschätzung ist es immer eine gute Maßnahme, die Betroffenen zu informieren, und zwar unabhängig von der Pflicht bzw. der Risikogewichtung. Neben Offenheit / Transparenz besteht gleichzeitig die Möglichkeit, nach der Risikoeinschätzung der Betroffenen aus einem möglichen Datenverlust zu fragen.
- Wiederholung vermeiden: Können Maßnahmen ergriffen werden, um solche Vorfälle künftig zu vermeiden (!)?
- Dokumentation & Meldung: Sind 🟢 geringe bis keine Schäden zu erwarten (z. B. fehlgeleitete Einladungsmail) sollte der Vorgang in einer kurzen Notiz mit den getroffenen Maßnahmen festgehalten werden. Ab einem zu erwartenden 🟡 mittleren Risiko besteht Meldepflicht gegenüber der zuständigen Aufsichtsbehörde und bei zu erwartendem 🟠 hohen Risiko die Pflicht zur Information der Betroffenen. Eine kurze Zusammenfassung (1. Seite) zur „Meldung einer Schutzverletzung"[2] und eine Checkliste zum Ausfüllen und Erstellung einer Meldung an die Aufsichtsbehörde einschließlich zur eigenen Dokumentation[3] finden Sie auf meiner Website.

ii) Für den Empfänger[4]

Da es für eine weitere Verarbeitung von fehlgeleiteten, personenbezogenen Daten weder einen Zweck (Sinn) noch eine Rechtsgrundlage gibt, spricht aus Sicht des Datenschutzes nicht gegen eine Löschung (und Bestätigung).

Werden die Daten allerdings (natürlich) versehentlich selbst in eigenen Systemen verarbeitet, fällt dies möglicherweise unter die Aufbewahrungspflichten der Abgabenordnung §147 AO oder §257 HGB. Der Rechtsgrund der Verarbeitung ergibt sich dann aus Art.6 Abs.1c DS-GVO mit einer Löschfrist nach Art.17 Abs.3b. Nach den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) lautet es unter 11.2 (Nr. 172):[5]

> *Enthalten elektronisch gespeicherte Datenbestände z. B. nicht aufzeichnungs- und aufbewahrungspflichtige, personenbezogene oder dem Berufsgeheimnis (§102 AO) unterliegende Daten, so obliegt es dem Steuerpflichtigen oder dem von ihm beauftragten Dritten, die Datenbestände so zu organisieren, dass der Prüfer nur auf die aufzeichnungs- und aufbewahrungspflichtigen Daten des Steuerpflichtigen zugreifen kann. Dies kann z. B. durch geeignete Zugriffsbeschränkungen oder „digitales Schwärzen" der zu schützenden Informationen erfolgen. Für versehentlich überlassene Daten besteht kein Verwertungsverbot.*

Handelt es sich mit der eigenen Verarbeitung also um nicht aufzeichnungs- bzw. aufbewahrungspflichtige Daten / Unterlagen, können diese gelöscht bzw. vernichtet werden. Zur Sicherheit kann eine neutrale Notiz dazu nicht schaden. In allen anderen Fällen sollten die Daten zu Personen bzw. Berufsgeheimnissen gezielt gelöscht und unkenntlich gemacht werden, auf jeden Fall sind diese für die weitere Verarbeitung zu sperren, Zugriffsrechte zu minimieren und nach Ablauf der gesetzlichen Aufbewahrungsfrist direkt zu löschen.

3. Zur Datensicherheit

(a) Doxing?

Immer wieder faszinierende neue Wortkreation, oder? In dem Wort steckt die Abkürzung für

1 Quelle: DSK: „Kurzpapier Nr. 18 „Risiko für die Rechte und Freiheiten natürlicher Personen""
2 LINK: Datenschutzverletzung – Information (12/2022) - PDF
3 LINK: Vorlage Checkliste und Meldung (12/2022) - PDF
4 Quelle: Dr.Datenschutz: „Fehlversand: Wie umgehen mit aufgezwungenen Daten"
5 Quelle: BMF Amtliches AO-Handbuch

CC BY SA

Dokumente / Documents und bezeichnet das Zusammentragen von veröffentlichten, personenbezogenen Daten im Internet mit unterschiedlichen und zum Teil auch kriminellen Absichten (LKA-NRW).[6] Zunehmend rücken Identitäten von Privatpersonen und Mitarbeiter*n mit Zugriff auf Firmendaten in den Fokus von Cyberkriminellen. Jetzt sitzen Hacker nicht wie in Film, Fernsehen und Bildern als dunkle Gestalt stundenlang vor ihrem Rechner und versuchen im „Trial-and-Error“ Verfahren Passwörter zu knacken. Das dauert zu lange und ist viel zu umständlich, einfacher ist die Manipulation zur Herausgabe bei Personen. Der Schaden 2023 aus Cyberbetrugsfällen beläuft sich laut Statista auf 206 Mrd. Euro und davon 16,1 Mrd. Euro auf Erpressung.[7]

i) Vorgehen

Heute ist es ein leichtes, Information über das Internet und Social-Media-Plattformen zu einer Person zusammenzutragen. Mittels millionenfach verschickter E-Mails, Textnachrichten oder Anrufen sammeln sie (konkret oder per Zufall) weitere Daten. Sind ausreichende Informationen vorhanden, wird mit den verschiedenen Methoden versucht (in den meisten Fällen Phishing, auch in Verbindung mit gefälschten Webseiten wie paypal oder Banken) an Anmeldedaten zu kommen, um Konten abzugreifen oder Bestellungen zu platzieren und die Ware oder das Geld abzugreifen. Eine perfide Methode ist auch, Mitarbeiter von Unternehmen unter Druck zu setzen, um Zugangsdaten freizugeben und/oder Zahlungen in beträchtlicher Höhe zu veranlassen (z. B. Chefbetrug).

Bereits Online gestohlene Passwörter können im Darknet auch dazugekauft werden. Da Nutzer nicht immer neue Passwörter vergeben, nutzen Kriminelle verschiedene Tools, um Datenbanken mit gestohlenen Passwörtern zu durchforsten und zu prüfen, ob die Anmeldedaten für den Zugriff auf andere Konten verwendet werden können.

ii) Schutz

Natürlich ist mit veröffentlichten Daten sparsam umzugehen. Mit einem Passwortmanager bestehen zwei Vorteile, neben der Generierung eines starken Passworts, speichert dieser auch die korrekte Adresse der Webseite. Zusatzschutz für wichtige Zugänge (Bezahlfunktionen oder vertrauliche Daten) ist die Zwei-Faktor-Authentifizierung z. B. über das Smartphone oder einen Token, da nutzten dem Hacker auch Benutzername und Passwort nichts. Für Firmenzugänge bietet sich auch das Passwort Hashing an, dabei werden die Passwörter in der Firmenumgebung nur in verschlüsselter Form (Hash) gespeichert. Beim Anmelden wird das Passwort sofort in den Hash-Wert gewandelt und mit der Firmendatenbank verglichen, so fällt es Hackern schwer, auf dem Firmensystem die Passwörter zu entschlüsseln. „Nichtsdestotrotz“ ist mit offenen Augen vor Gefahren durch das Cyberspace zu gehen.

4. Zu angrenzenden Themen

(a) Wie kommen die an meine Daten?

Aufgrund vieler Bürgeranfragen hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg eine FAQ – Liste zur berechtigten Weitergabe von Daten der Meldebehörden zusammengestellt, die über diesen LINK aufgerufen werden kann. Dort werden z. B. Antworten auf Fragen zu Wahlwerbungen, Jubiläumsbriefen, Telefonbucheinträgen, Informationsmaterialien zur Bundeswehr u.ä. gegeben.

Bei Bedarf, einfach mal sprechen!

6 *Quelle: LKA-NRW. „Nutzer machen es den Hackern oft viel zu leicht“*
7 *Quelle: Statista Research: „Schäden durch Angriffe in Deutschland 2023“*