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

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) Erlaubte Auskünfte bei Anmietung?

Die Datenschutzkonferenz, die Aufsichtsbehörden des Bundes und der Länder haben eine überarbeitete Version der Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressent:innen[1] veröffentlicht und dabei eine sehr schöne Unterteilung vorgenommen:

i) Zum Besichtigungstermin

- ✔ Angaben zur Identifikation, wie vollständiger Name und Anschrift, einschließlich Sichtung des Personalausweises (Kopien sind nicht erforderlich, siehe auch §20 Personalausweis – Gesetz).
- ✔ Angaben zu Wohnberechtigungsschein, sofern für die Anmietung erforderlich

ii) Zum Anmietungsinteresse

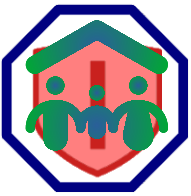
- ✔ Familienstand und Angaben zu den im Haushalt lebenden Personen (Erwachsene und Kinder) und zu Haustieren, sofern es sich nicht um Kleintiere handelt.

1 *Quelle: DSK: „Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressent:innen“ PDF*

- ✔ Ausgeübter Beruf und derzeitiger Arbeitgeber.
- ✔ Angaben zum Einkommen (Angaben, nicht Bescheinigungen), monatliches Nettoeinkommen bzw. der Betrag, der nach laufenden Belastungen für die Miete zur Verfügung steht. Oder die Frage, ob ein bestimmter Betrag (Ja/Nein) monatliche zur Verfügung steht.
- ✔ Frage (Ja/Nein) zu Insolvenzverfahren und möglichen Räumungstiteln.

iii) Zum Abschluss des Mietvertrages

- ✔ Nachweis zum monatlichen Nettoeinkommen (nicht benötigte Angaben schwärzen ist erlaubt) und Nachweis der wirtschaftlichen Bonität, oder Einholung einer Auskunft durch den Vermieter, sofern dies erforderlich ist.
- ✔ Wurden in den letzten 2 Jahren Mietzahlungspflichten verletzt (Ja/Nein) und/oder wurden vergangene Mietverhältnisse rechtswirksam gekündigt (Ja/Nein) und wenn ja die Gründe und mögliche Begründung, dass dies nicht vorkommen wird.
- ✔ Vorstrafen und strafrechtliche Ermittlungsverfahren



iv) „Eigentlich" nicht erlaubt

Nicht nur „eigentlich", es besteht die Gefahr von rechtlichen Risiken bzw. rechtlichen Möglichkeiten, je nach Betrachtungsweise.

- ✗ Weitere Auskünfte über die jeweiligen Punkte zu i bis iii sind nicht erlaubt.
- ✗ Keine Forderung nach gesamtschuldnerischer Haftung von Ehepartnern.

(PS: Mitunterschrift als Mieter schützt vor Kündigung, falls der Hauptmieter auszieht u. ä.)

- ✗ Kein Fragen nach Religion, Rasse, ethnischer Herkunft bzw. Staatsangehörigkeit (§19 AGG Zivilrechtliches Benachteiligungsverbot). Ausnahmen bestehen bei vorliegendem, schlüssigem, wohnungspolitischem Gesamtkonzept, sofern dies zur Schaffung und Erhaltung sozialer und stabiler Bewohnerstrukturen, ausgewogener Siedlungsstrukturen sowie ausgeglichener wirtschaftlicher, sozialer und kultureller Verhältnisse notwendig ist.
- ✗ Unzulässige Fragen sind auch die nach Heiratsabsichten, Schwangerschaften, Kinderwünschen oder Mitgliedschaften in Parteien und Mietvereinen.
- ✗ Verboten ist die Speicherung zur Führung von „schwarzen Listen", z. B. von auffälligen Mietern.

v) Hinweise

- ➢ Die Abfrage von Bonitätsauskünften über Mietinteressent:innen bei Auskunfteien ist nur dann zulässig, wenn die Voraussetzungen einer gesetzlichen Vorschrift (Art.6 Abs.1b/f DS-GVO) erfüllt sind. Liegen bereits ausreichende Informationen über die Bonität der Mietinteressent:innen vor, z. B. durch spezielle Bonitätsnachweise, ist eine Abfrage bei Auskunfteien durch Vermieter:innen nicht zulässig. Eine „freiwillige Einwilligung" schließt sich in diesem Fall aus.
- ➢ Entfällt der Zweck einer Anfrage, weil kein Mietvertrag abgeschlossen wurde, sind diese Daten umgehend zu löschen, da der Zweck der Erhebung und Speicherung entfallen ist. Die Löschung sollte spätestens (oder vorsichtshalber) nach 6 Monaten erfolgen, wenn Ansprüche aus §21 AGG Ansprüche nicht mehr zu erwarten sind. Es besteht die Möglichkeit zur freiwilligen Einwilligung in die weitere Speicherung von Kontaktdaten für die Kontaktaufnahme bei frei werdenden Wohnungen.
- ➢ Muster zur Einholung von (Selbst-) Auskünften sind der Orientierungshilfe der DSK angehängt.

3. Zur Datensicherheit

Wegen der (noch) sehr weiten Verbreitung von Microsoft / Windows und Google / Android ist hier oft zu Bugs von Microsoft und Android zu lesen, aber Apple (wie auch Linux) holen kontinuierlich Marktanteile auf. Das macht es für Hacker auch interessant, da diese auch wirtschaftlich denken. Deswegen mal hier zu Apple: Die einen sagen: ‚Apple – Produkte' brauchen keinen zusätzlichen Schutz", die anderen schlagen die Hände über dem Kopf zusammen (meist IT – Verantwortliche in Unternehmen).

Jamf, ein Anbieter für Mobile-Device-Management-Lösungen für Apple Produkte, hat seinen Jahresbericht zur Sicherheit zu Apple – Systemen veröffentlicht („Security 360: Annual Trends Report 2024“[2]) mit Stichproben von 15 Millionen Desktop-Computern, Tabletts und Smartphone-Geräten, die sie schützen, in 90 Ländern und mehreren Plattformen (macOS, iOS/iPad, Android und Windows).

Die Fakten sind:

- 40 % der mobilen Nutzer und 39 % der Unternehmen betreiben ein Gerät mit bekannten Angriffsmöglichkeiten (z. B. fehlende Sicherheitsupdates)
- Jamf verfolgt 300 Malware - Familien auf macOS und hat in 2023 dazu 21 neue Malware - Familien auf dem Mac gefunden.
- Trojaner werden immer beliebter und machen 17 % aller Mac – Malware - Instanzen aus.
- 20 % der Organisationen wurden von böswilligem Netzwerkverkehr betroffen. Die Ergebnisse des Berichts sind in vier Bedrohungskategorien unterteilt: Anwendungsrisiken, Malware - Risiken, Angriffsentwicklung und webbasierte Risiken.
- Phishing-Versuche waren auf mobilen Geräten 50 % erfolgreicher als auf Macs

Dazu passt die Meldung von heise-online: *„macOS 14.4 und mehr: Apple patcht schwere Sicherheitslücken“*[3]. Natürlich gibt es noch deutlich mehr Schädlinge unter Windows und Android, aber es werden eben auch für Apple stetig mehr. Dabei helfen klassische Sicherheitsregeln, wie regelmäßige Updates, gute Passwörter und 2-Faktor-Authentifizierung über alle Systeme viel Probleme zu vermeiden.

4. Zu angrenzenden Themen

(a)Mythen zur 2-Faktor-Authentifizierung

So der Titel aus einem Interview von WIRED mit Jim Fenton, CSO bei OneID und verantwortlich für die Sicherheitsgestaltung des OneID – Identitätssystems, sowie die Aufsicht über die Unternehmenssicherheit.[4]

- **„DIE Lösung“:** Die Zwei-Faktor-Authentifizierung verbessert die Sicherheit, aber es ist nicht die Lösung in allen Fällen. Die Annahme der falschen 2FA-Lösung kann Benutzer mit geringem Sicherheitsvorteil belasten. Ihre Benutzer und die Sicherheitsbedrohungen zu verstehen, denen Sie ausgesetzt sind, ist der Schlüssel zu einer erfolgreichen Zwei-Faktor-Authentifizierungsbereitstellung.
- „**Die schnelle Lösung** bei einer Verletzung ist das Einschalten der 2FA“. Wenn es nur als Option angeboten wird, machen die meisten Nutzer sich nicht die Mühe, um sich unabhängig von den Sicherheitsfaktoren anzumelden, da ein zweites Gerät, oder das Einbetten eines kryptischen Schlüssels erforderlich ist.
- **„Nicht anfällig für Bedrohungen“**: Während die Zwei-Faktor-Authentifizierung die Sicherheit verbessert, ist sie nicht perfekt und zieht Angreifer an, weil sie hauptsächlich für hochwertige Anwendungen verwendet wird. Für einen Hacker ist es noch zu einfach, einem unaufmerksamen Benutzer eine vom Angreifer angestoßene Transaktion zu genehmigen. Übrigens, SMS ist unverschlüsselt und lässt sich leichter manipulieren.
- **„2FA = 2 Geräte“**: Wenn Benutzer zu intelligenteren persönlichen Geräten wechseln, ist es praktischer geworden, Schlüsselinformationen in diese Geräte zu laden, die manipulationssicher genug sind, um ein hohes Maß an Sicherheit zu bieten.

Bei Bedarf, einfach mal sprechen!

2 *Quelle: Jamf Holding Corp.: „Security 360: Annual Trends Report 2024“*
3 *Quelle: heise-online: „macOS 14.4 und mehr: Apple patcht schwere Sicherheitslücken“*
4 *Quelle: WIRED: „5 Mythos of two-facotor authentication“*