Übersicht 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.

HINWEISE:

Das Inhaltsverzeichnis finden Sie ab Seite 2:

- ✔ Die Einzelthemen können Sie mit einem Mausklick in der Inhaltsangabe direkt ansteuern
- ✔ Mit der Suche <Strg + F> können Sie auch Ihr Thema direkt finden
- ✔ Quellenangaben <NR.> sind hier statt als Fußnote als Endnote (letzte Seiten) aufgeführt und mit einem <Klick auf NR.> zu erreichen. Es macht dieses Jahresarchiv übersichtlicher.
- ✔ Die Quellenangaben können über einen Mausklick auf die Fußnote direkt angesteuert werden.

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	**Bundesdatenschutz-gesetz** 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 technischen - organisatorischen Maßnahmen zur Unterstützung der Transformation abstrakter – rechtlicher Anforderungen in konkrete Maßnahmen. Ziel ist, eine gemeinsame Sprache der Informatiker und Juristen für die Verantwortlichen und Datenschutzpraktiker zu finden. | SDM Version 3.0 (12/2022)* | 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).*

Inhalte ➔ MM@2024

➔ 01@2024

(2) Zum Datenschutz

(a) Das E-Rezept

i) Wer ist „gematik“

Die Bundesrepublik Deutschland (Bundesministerium für Gesundheit) ist im Mai 2019 als Mehrheitsgesellschafter mit 51 % in die gematik GmbH eingetreten[1]. Weitere Gesellschafter sind die jeweiligen Spitzenverbände der Ärzte, Apotheken und Krankenhäuser. Der gesetzliche Auftrag der gematik umfasst die Einführung, den Betrieb und die Weiterentwicklung der sicheren Telematik – Infrastruktur im Gesundheitswesen, für Fachanwendungen und weiterer Anwendungen für die Kommunikation zwischen Heilberuflern, Kostenträgern und Versicherten.[2]

ii) Wie geht „E-Rezept“

Grundvoraussetzung ist die Gesundheitskarte, deren Daten gesichert über die jeweilige Krankenkasse verwaltet werden und bei jedem Arztbesuch pro Quartal vorzulegen bzw. einzulesen ist. Für die Einlösung des Rezeptes gibt es dann folgende Möglichkeiten

(a) Das Rezept wird auf Papier mit QR-Codes gedruckt und ist in der Apotheke vorzulegen.

(b) Das Rezept wird auf über die G-Karte gespeichert und von der Apotheke ausgelesen

(c) Das Rezept wird in der eingerichteten E-Rezept-App abrufbar und kann von der Apotheke ausgelesen werden (Smartphone mit NFC - Funktion)
[*Vor dem ersten Einsatz ist im ersten Schritt die App der Krankenkasse zu installieren und das Identifikationsverfahren zu durchlaufen. Im zweiten Schritt ist die E-Rezepte-App zu installieren und mit der Krankenkassen-App über das Anmelde-Prozedere zu verbinden. Nach dem einmaligen Einrichten können die Rezepte in der App abgerufen und eingelöst werden*]

In allen Fällen sind die Daten in der sicheren Telematik – Infrastruktur gespeichert. Weitere Vorteile bei dem Gebrauch der Gesundheitskarte (b) ist die Möglichkeit von Folgerezepten ohne Praxisbesuch und mit der E-Rezept-App (c) können zusätzlich Angehörige mitverwaltet werden.[3]

iii) Datenschutz und E-Rezept

Jetzt ist Datenschutz und -sicherheit hier nicht in der Kürze zu beantworten. Der wissenschaftliche Dienst des Deutschen Bundestages hat dazu ein Kurzgutachten[4] über 148 Seiten erstellt und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat eine FAQ zum E-Rezept[5] wegen der vielen Anfragen veröffentlicht. Einige Punkte daraus:

- Die in der Praxis erstellten E-Rezepte werden deutschlandweit in einem zentralen System über eine „Ende-zu-Ende“ Verschlüsselung übertragen, gespeichert und mit entsprechenden Maßnahmen gesichert. Betreiber / Fachdienst ist die IBM Deutschland GmbH. „*Dem BfDI liegen keine Erkenntnisse vor, dass die in den Anforderungen der gematik formulierten Maßnahmen nicht wirksam sind*“.
- Nach den Vorgaben werden die E-Rezepte für maximal 100 Tage gespeichert.
- Auf die Daten zugreifen können Ärzte, Zahnärzte, Psychotherapeuten und Apotheker, die in die Behandlung eingebunden sind, wenn dies für die Versorgung erforderlich ist. Eine gesonderte Einwilligung des Versicherten ist also nicht erforderlich, da – zumindest für die Behandlung – gesetzliche Grundlagen für die Verarbeitung von Gesundheitsdaten greifen. Die Rechtmäßigkeit der Verarbeitung (Art.6 Abs.1c DS-GVO, rechtliche Verpflichtung) ist in §360ff Sozialgesetzbuch (V) geregelt.
- Versicherte müssen das E-Rezept auch dann nutzen, wenn sie kein Smartphone oder die E-Rezept-App haben. Sie können ihre Gesundheitskarte zur Einlösung nutzen oder sich einen QR - Code ausdrucken lassen. Die Daten sind allerdings auch in der Telematik - Infrastruktur vorhanden.
- Versicherte haben die Möglichkeit, das E-Rezept, die zugehörigen Rechnungsdaten und Informationen freiwillig in ihrer elektronischen Patientenakte (ePA) zu speichern. In diesem Fall ist eine Einwilligung erforderlich. Die ePA steht seit 2021 zur Verfügung und wird 2025 für alle

gesetzlich Versicherten bereitgestellt. Zudem ist geplant, die Daten aus der ePA pseudonymisiert für Forschungszwecke zu nutzen. Der Nutzung der ePA und der Verarbeitung der ePA-Daten zu Forschungszwecken muss aktiv widersprochen werden.

Um dem Ruf nach „Digitalisierung“ nachzukommen, sind die im Rahmen der DS-GVO möglichen Einschränkungen der allgemeinen Rechte zum Datenschutz durch gesetzliche Grundlagen bei besonderen Gegebenheiten wohl zu akzeptieren.

(b) Transkription und Datenschutz

In diversen Konferenzanwendungen werden sukzessive auch Werkzeuge zur Transkription (Aufzeichnung des gesprochenen Wortes) angeboten. Stellt sich sofort die Frage nach der Erlaubnis unter Datenschutzgesichtspunkten.

Zunächst gibt es da noch den §201 StGB[6] Verletzung der Vertraulichkeit des Wortes, danach ist strafbar, wer nicht öffentlich gesprochene Worte auf Tonträger aufnimmt und Dritten zugänglich macht. Der „Tonträger“ ist vielleicht ein wenig aus der Zeit geraten, aber spätestens bei der digitalen Ablage ist man aber schon sehr dicht dran.

Bei Telefonaufzeichnungen hat die Datenschutzkonferenz[7] eine klare Meinung. Vor Aufzeichnung muss die Einwilligung nachweisbar in informativer Weise und freiwillig von jedem Teilnehmer erfolgen. Nur auf ein berechtigtes Interesse des Konferenzanbieters (Einladende/r) als Rechtsgrundlage zu setzen, ist so gut wie ausgeschlossen. Bei Mitarbeitern ist der Nachweis der Freiwilligkeit (Abhängigkeitsverhältnis) nicht ganz so einfach nachzuweisen.

i) Personenbezogene Daten?

Gute Frage! Jetzt sind es ja nur schriftliche Aufzeichnungen ohne Ton (biometrische Daten). Unterstellt, es werden bei einer Webkonferenz auch keine Namen und keine Bilder der Aufzeichnung hinzugefügt, so besteht doch die Möglichkeit auf Basis des Themas und des Inhalts einzelne Aussagen Personen zuzuordnen. Damit sind es keine anonymisierten, sondern pseudonymisierte Daten. Deshalb sollte bei einer Webkonferenz im Vorfeld eine nachweisbare Einwilligung unter Einschluss einer möglichen Weitergabe an Dritte (sofern vorgesehen) eingeholt werden. *(PS: Heimliche Aufzeichnungen von Gesprächen verbieten sich damit von selbst!)*

ii) Checkliste am Beispiel für ein Interview:

(a) Alle involvierten Personen sind auf Datenschutz und -geheimnis zu verpflichten. Dem Merkblatt „Datenschutz für Mitarbeiter“[8] ist eine Mustererklärung als Anlage beigefügt.
(b) Vorbereitung und Einholung der Einwilligungserklärung vor dem Gespräch (Muster[9]).
(c) Aufzeichnung, Übertragung und Speicherung müssen auf gesichertem Wege erfolgen, nach dem Stand der Technik, so die DS-GVO (z.B. verschlüsselt, mit Zugriffsschutz und wenn auf Servern / Cloud möglichst nur innerhalb der EU oder einem sicheren Drittland).
(d) Bei Einschaltung eines Dienstleisters (mit Übertragung der Daten) sollte die konforme Datenschutzverarbeitung durch einen Auftragsverarbeitungsvertrag gesichert sein.
(e) Ein gesichertes Löschkonzept ist festzulegen. Wenn der Zweck entfällt, ist das Transkript sicher zu löschen. Information über „wie endgültig löschen“ stellt das BSI zur Verfügung.[10]
(f) Wichtig zum Nachweis ist auch die Dokumentation der ergriffenen Maßnahmen.
(g) Und sollte etwas schiefgehen, nicht die Informationspflichten des Betroffenen vergessen!

Bei Webkonferenz empfiehlt es sich bei Aufzeichnungen einen Blick in die Einstellungen zu werfen. Mit richtigen Einstellungen kann schon viel verhindert werden.

(3) Zur Datensicherheit

(a) Hackerangriff auf Trello

Trello ist ein auf Kanban basierender Aufgaben-Verwaltungs-Onlinedienst des Unternehmens Atlassian. Wie die Netzwelt[11] berichtet, haben Hacker Daten von über 15 Millionen User von Trello erbeutet, deshalb Zugangsdaten ändern und prüfen, ob die Daten im Netz angeboten werden.

(4) Zu angrenzenden Themen

(a) Skrupellos! Kriminelle Maschen: Tatort Internet

Anschaulich für alle, die immer ‚*nichts zu verbergen haben*' und meinen dadurch für Hacker uninteressant zu sein". Link: zdf-info, Video 43 Min. (Klick and run).

➔ 02@2024

(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 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.[12]
- ✔ 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"[13] und eine Checkliste zum Ausfüllen und Erstellung einer Meldung an die Aufsichtsbehörde einschließlich zur eigenen Dokumentation[14] finden Sie auf meiner Website.

ii) Für den Empfänger[15]

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).

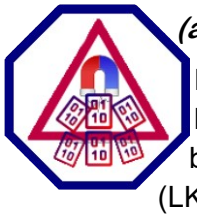
Werden die Daten allerdings (natürlich) versehentlich selbst in eigenen Systemen verarbeitet, fällt dies möglicherweise unter die Aufbewahrungspflichten der Abgabenordnung §147 AO oder §257 HGB. Der Rechtsgrund der Verarbeitung ergibt sich dann aus Art.6 Abs.1c DS-GVO mit einer Löschfrist nach Art.17 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):[16]

Enthalten elektronisch gespeicherte Datenbestände z. B. nicht aufzeichnungs- und aufbewahrungspflichti-

ge, 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 Dokumente / Documents und bezeichnet das Zusammentragen von veröffentlichten, personenbezogenen Daten im Internet mit unterschiedlichen und zum Teil auch kriminellen Absichten (LKA-NRW).[17] 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.[18]

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.

➔ 03@2024

(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[19] veröffentlicht und dabei eine sehr schöne Unterteilung vorgenommen:

i) Zum Besichtigungstermin

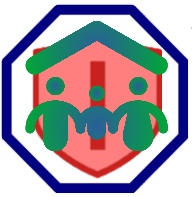
- ✔ Angaben zur Identifikation, wie vollständiger Name und Anschrift, einschließlich Sichtung des Personalausweises (Kopien sind nicht erforderlich, siehe auch §20 Personalausweis – Gesetz).
- ✔ Angaben zu Wohnberechtigungsschein, sofern für die Anmietung erforderlich

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.
- ✔ 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) monatlich 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

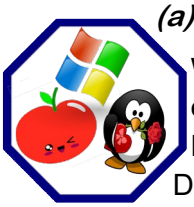
- ➢ Die Abfrage von Bonitätsauskünften über Mietinteressent:innen bei Auskunfteien ist nur dann zulässig, wenn die Voraussetzungen einer gesetzlichen Vorschrift (Art.6 Abs.1b/f DS-GVO) erfüllt sind. Liegen bereits ausreichende Informationen über die Bonität der Miet-

interessent: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

(a) Die Sache mit: „Apple ist sich(er)er“?!



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“[20]) 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“*[21]. 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 viele 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.[22]

- **„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.

➔ 04@2024

(2) Zum Datenschutz

Bei Bedarf, einfach mal sprechen! 

ENDNOTEN NR.

1 Quelle: https://www.gematik.de/ueber-uns/struktur
2 Quelle: https://www.gematik.de/ueber-uns/gesetzliche-grundlagen
3 Quelle: https://www.gematik.de/anwendungen/e-rezept/versicherte
4 Link: Wissenschaftlicher Dienst des Bundestages: „Kurzgutachten Elektronische Patientendaten und Telematikinfrastruktur“
5 Link: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: „FAQ zum E-Rezept“
6 Quelle: dejure.org: §201 StGB „Verletzung der Vertraulichkeit des Wortes“
7 Quelle: DSK Beschluss 23.03.2018: „Aufzeichnung von Telefongesprächen“ (PDF)
8 Quelle: https://volkerschroer.de/DSGVO/2021.02.26.Mitarbeiter.Merkblatt.pdf
9 Muster: „Einwilligungserklärung Uni Siege“ Universität Marburg Einverständniserklärung (PDF)
10 Quelle: BSI „Daten auf Festplatten und Smartphones endgültig löschen“
11 Quelle: Netzwelt: „Hackerangriff auf Trello: Daten von über 15 Millionen Usern erbeutet“
12 Quelle: DSK: „Kurzpapier Nr. 18 „Risiko für die Rechte und Freiheiten natürlicher Personen““
13 LINK: Datenschutzverletzung – Information (12/2022) - PDF
14 LINK: Vorlage Checkliste und Meldung (12/2022) - PDF
15 Quelle: Dr.Datenschutz: „Fehlversand: Wie umgehen mit aufgezwungenen Daten“
16 Quelle: BMF Amtliches AO-Handbuch
17 Quelle: LKA-NRW. „Nutzer machen es den Hackern oft viel zu leicht“
18 Quelle: Statista Research: „Schäden durch Angriffe in Deutschland 2023“
19 Quelle: DSK: „Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressent:innen“ PDF
20 Quelle: Jamf Holding Corp.: „Security 360: Annual Trends Report 2024“
21 Quelle: heise-online: „macOS 14.4 und mehr: Apple patcht schwere Sicherheitslücken“
22 Quelle: WIRED: „5 Mythos of two-facotor authentication“