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 *(Einfach Thema mit <Strg+F> suchen, oder direkt hier anklicken)*

➔ 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]

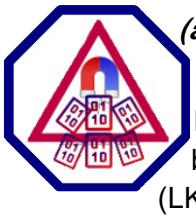
Da es für eine weitere Verarbeitung von fehlgeleiteten, personenbezogenen Daten weder einen Zweck (Sinn) noch eine Rechtsgrundlage gibt, spricht aus Sicht des Datenschutzes nicht gegen eine Löschung (und Bestätigung).

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 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 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

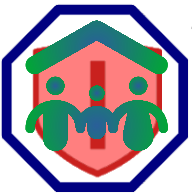
- ✔ Angaben zur Identifikation, wie vollständiger Name und Anschrift, einschließlich Sichtung des Personalausweises (Kopien sind nicht erforderlich, siehe auch §20 Personalausweis – Gesetz).
- ✔ Angaben zu Wohnberechtigungsschein, sofern für die Anmietung erforderlich

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

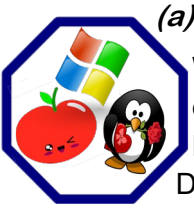
- ➢ Die Abfrage von Bonitätsauskünften über Mietinteressent:innen bei Auskunfteien ist nur dann zulässig, wenn die Voraussetzungen einer gesetzlichen Vorschrift (Art.6 Abs.1b/f DS-

GVO) erfüllt sind. Liegen bereits ausreichende Informationen über die Bonität der 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

(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

(a) Die Sache mit dem „berechtigten Interesse“[23]

Für jede Verarbeitung von personenbezogenen Daten gilt es eine Rechtsgrundlage vorzuweisen, so schreibt es Art.6 Abs.1 DS-GVO vor. Da wären die Einwilligung (1a), Vertragserfüllung (1b), rechtliche Verpflichtungen (1c), lebenswichtige Interessen (1d), öffentliches Interesse (1e) und (1f) Wahrung der berechtigten Interessen des Verantwortlichen:

„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.“

Es entsteht der Eindruck, dass dieser Tatbestand sehr oft als rechtlicher Restposten oder Auffangbecken (geht zur Not immer) betrachtet wird.

i) TIPP dazu: Fernseher ☹

Wer ein wenig Zeit hat, sollte mal die Datenschutzeinstellung seines Fernsehers mit Internetanschluss anschauen, gerade wenn die generelle Frage zur „Einwilligung“ verneint wurde. Dass es ein „berechtigtes Interesse“ für Stabilität und Sicherheit zur Nutzung des Fernsehers gibt, ist mehr als verständlich. Aber die dahinter liegenden, vielfachen „berechtigten Interessen“ zielen beim näheren Hinsehen ausschließlich darauf ab, Werbung über das Nutzerverhalten zu generieren und die Standorte der Gesellschaften sind über den Globus verteilt. In weiser Voraussicht ist wohl eine einzelne Abwahl möglich – so auf unserem Fernseher -.

ii) Was ist „berechtigtes Interesse“?

So ganz eindeutig ist es in der Verordnung und dem Gesetz nicht definiert, aber es gibt Hinweise aus den Erwägungsgründen der DS-GVO (ErwG). So lautet es in ErwG (47)

„die vernünftigen Erwartungen der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen … beispielsweise … eine maßgebliche Beziehung … z.B. … ein Kunde … oder in seinen Diensten steht“. (Leider steht da auch) *... zum Zwecke der Direktwerbung kann als eine, einem berechtigten Interesse dienende Verarbeitung betrachtet werden.“*

Dank des Gesetzes gegen den unlauteren Wettbewerb und des Tele-Medien-Gesetzes muss die Möglichkeit bestehen, diese Sammlung zu unterbinden (PS: Allerdings war es jetzt am Fernseher mühsam, jeden einzelnen abzuwählen). ErwG (48) enthält ein „kleines Konzernprivileg“ dazu, bezüglich der Verarbeitung innerhalb einer zentrierten Unternehmensgruppe, allerdings nicht über Grenzen hinweg. ErwG (39) besagt, dass personenbezogene Daten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch mildere Mittel erreicht wird.

iii) Aber: Die Abwägung ist zwingend

Der Schutz und die Grundfreiheiten der betroffenen Person dürfen nicht überwiegen. Deshalb ist eine Abwägung mit dem berechtigten Interesse des Verantwortlichen (Datenverarbeiter) zwingend vorzunehmen und zu dokumentieren. Die abzuwägenden Gründe sind in der DS-GVO leider nicht benannt. Anhaltspunkte sind:

- Art.7 der EU Charta der Grundrechte: „Achtung des Privat- und Familienlebens“
- Art.8 der EU Charta der Grundrechte: „Schutz der personenbezogenen Daten“, u. a. „nur nach Treu und Glauben, festgelegte Zwecke, Einwilligung, Auskünfte“.
- ErwG (47), die vernünftige Erwartung der betroffenen Personen
- Sowie aus den Vorschriften der DS-GVO, wie Quelle, Menge und Art der Daten, Dauer- und Sicherheit der Verarbeitung und die Anzahl der involvierten Datenverarbeiter.

Fazit: Eine offene und faire Information ist der beste Schutz vor Auseinandersetzungen.

iv) Falschparken und Datenschutz?

Dieser Zusammenhang hat mich auch überrascht, zumal es im Videobeitrag des WDR („Immer mehr Bürger zeigen Falschparker an“)[24] nicht angemerkt wird, sondern nur im Text verlinkt ist. DAS können sich m. E. auch nur Rechtsanwälte ausdenken.

Wie der ADAC veröffentlicht[25], bekam der Fotograf / Anzeigenerstatter zunächst eine Verwarnung des Bay. Landesamtes für Datenschutzaufsicht über € 100,--. Dagegen klagte dieser vor dem Verwaltungsgericht Ansbach und bekam Recht. Im Urteil VG Ansbach, Urteil v. 02.11.2022 – AN 14 K 22.00468[26] lautet es unter 6. und hier kommt das *„berechtigte Interesse“* ins Spiel:

> *6. Dient die Übermittlung personenbezogener Daten an eine Polizeiinspektion als zuständige Behörde im Sinne des Erwägungsgrundes 50 der DS-GVO dem Hinweis auf eine begangene Ordnungswidrigkeit, so besteht ein berechtigtes Interesse an der Datenverarbeitung, welches grundsätzlich eine Verarbeitung personenbezogener Daten i.S.d. Art. 6 I 1 Buchst. f DS-GVO rechtfertigen kann. (Rn. 69) (redaktioneller Leitsatz)*

Laut WDR wird in NRW sogar aufgefordert, Falschparken inklusive Foto anzuzeigen.

Fazit: Erlaubt sind Fotos mit Nummernschild (personenbezogene Daten) unter Angabe der Kontaktdaten. Allerdings sollten keine unbeteiligten Personen wie Fahrzeuge erkennbar sein.

(b) LibreOffice statt Microsoft Office geht das?

Es wird spannend zu beobachten, denn LibreOffice[27] und die Landesregierung Schleswig-Holstein[28] verkünden den „Einstieg in den Umstieg“. Die Datenschutzaufsichtsbehörden waren und sind von Anfang an eher skeptisch gegenüber der Erfüllung der Datenschutzanforderungen durch Microsoft Office. Es reicht von Tipps zu den Verträgen (Aufsicht Niedersachsen) über Warnungen (Aufsicht Bayern) bis zum – mehr oder weniger – Verbot (Aufsicht Hamburg). Die Ankündigung und deren Umsetzung durch Schleswig-Holstein ist ein erster großer Schritt zu einer Alternative. Die Begründung ist auch nachvollziehbar:

> *Wir haben als Land eine große Verantwortung gegenüber unseren Bürgerinnen und Bürgern sowie Unternehmen, dass ihre Daten bei uns sicher aufgehoben sind und wir müssen sicherstellen, dass wir jederzeit Herr über unsere eingesetzten IT-Lösungen sind und wir als Staat unabhängig agieren können.*

(c) OpenStreetMap statt Google.Maps

Wie „DerWesten“[29] berichtet, stellt DHL die Sendungsverfolgung von Google Maps auf OpenStreetMap um, weil (so DHL):

> *„Es geht DHL um den Schutz der Kundendaten, der Wechsel von Google Maps zu OpenStreetMap ist nur ein Teilschritt auf dem Weg zur „digitalen Souveränität und Datenschutz“.*

(3) Zur Datensicherheit

(a) Die Sache mit „Linux ist sicher“

Dass die Betriebssysteme Windows und Android Maßnahmen zum Schutz gegen Hackerangriffe erfordern, ist weitläufig bekannt. Zu Apples Betriebssystem hatte ich im letzten Informationsbrief geschrieben. Das gleich gilt auch für Linux, so warnt beispielhaft das BSI aktuell vor einer gravierenden Sicherheitslücke in Linux[30]. Es ist keine Frage des

Betriebssystems, sondern dessen Verbreitung. Hacker denken effizient. Wenn die Chancen groß sind, lohnt sich der Aufwand. Da Alternativen zu Windows sich zunehmend verbreiten, lohnt sich auch der Aufwand. Wichtig ist bei allen eingesetzten Systemen auch den Schutz vor Angriffen nicht zu vergessen.

Das es auch Betriebssystem übergreifende Sicherheitsmeldungen gibt, zeigt die aktuelle Meldung „Acronis-Agent unter Linux, macOS und Windows verwundbar *(CVE-2024-34010, CVSS 8.2, Risiko "hoch")*“

(4) Zu angrenzenden Themen

(a) EuGH-Urteile zum Schufa-Score

Da kann ich aus einer Veröffentlichung der Commerzbank[31] einfach nur zitieren:

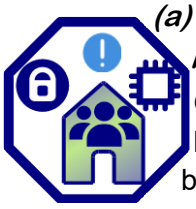
Zwei Fälle aus Deutschland haben den Europäischen Gerichtshof (EuGH) veranlasst, den Schufa-Score genauer unter die Lupe zu nehmen. Am 7. Dezember 2023 entschied der EuGH, dass das Schufa-Scoring künftig nicht mehr als alleinige Bewertung der Kreditwürdigkeit herangezogen werden darf. Ansonsten würde das Scoring der SCHUFA gegen die Europäische Datenschutzgrundverordnung (DSGVO) verstoßen: Denn wichtige Entscheidungen dürfen nach Artikel 22 der DSGVO nicht ausschließlich auf Basis automatisiert verarbeiteter Daten getroffen werden.

Bei einer automatisierten Entscheidung (Profiling) muss jedem auch ein persönlicher Ansprechpartner zur Verfügung gestellt werden. Und das gilt jetzt nicht nur für Kreditinstitute, sondern für alle anderen (z. B. Leasinggesellschaften, Telefongesellschaften, Vermieter u.s.w.).

➔ 05@2024

(2) Zum Datenschutz

(a) „Haushaltsausnahme“, was ist PRIVAT?



i) Fazit:

Grundsätzlich sind Privatpersonen von den Vorschriften der DSGVO befreit, es stellt aber keinen Freibrief dar und gilt nur, solange sie sich wirklich und ausschließlich im privaten Bereich bewegt. Bedeutet: *„Es kommt auf den Einzelfall an“*.

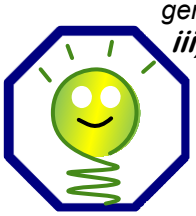
ii) Regelung DSGVO

Sachlicher Anwendungsbereich Art.2 Abs.2c DSGVO:

„Diese Verordnung findet keine Anwendung auf die Verarbeitung von personenbezogenen Daten ... durch natürlicher Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.“

Erwägungsgrund (18) DSGVO:

Diese Verordnung gilt nicht für die Verarbeitung von personenbezogenen Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird. Als persönliche oder familiäre Tätigkeiten könnte auch das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten gelten. Diese Verordnung gilt jedoch für die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen.



iii) ● Die DSGVO findet keine Anwendung ...

✔ … auf private Adress- und Telefonverzeichnisse (z. B. im Smartphone), sofern kein Bezug zu beruflicher oder wirtschaftlicher Tätigkeit besteht.

✔ … auf Social-Media-Accounts, wenn diese ausschließlich dem Zweck der Darstellung der eigenen Person dienen und ausschließlich im Rahmen persönlicher oder familiärer Tätigkeit erfolgt.

✔ … auf Urlaubsfotos, Videos und anderen Aufnahmen von Familie und Freunden, wenn diese ausschließlich diesem Personenkreis zur Verfügung stehen, worauf zu achten ist (! keine Bekannten von Bekannten des Personenkreises, wie in Einstellungen in Social-Media-Accounts).

iv) ***Die DSGVO findet Anwendung …***

✗ … bei Veröffentlichung an einen größeren Empfängerkreis außerhalb des persönlichen Umfeldes, z. B. Follower, Freunde und deren Follower und Freunde auf Social-Media-Accounts, oder eine Veröffentlichung auf Videoplattformen mit der Möglichkeit zu teilen. Bei virtuellem Freundeskreis und nicht exklusiven Followern wird es schwierig eine Abgrenzung zum persönlichen, familiären Kreis zu treffen bzw. diesen einzuhalten (Urteil EuGH C-345/17 Feb. 2019)[32]. Zur Vermeidung von Problemen sollte vorab eine Einwilligung der Beteiligten zur Veröffentlichung eingeholt werden (mündlich ausreichend, schriftlich besser nachweisbar).

✗ … insbesondere bei personenbezogenen Daten von Kindern bis 16 Jahre sollte vorab die Einwilligung der Eltern (m. E. auch im privaten, familiären Bereich), bzw. sollte vorab die Einwilligung der Erziehungsberechtigten nach Erwägungsgrund 38 i. V. m. Art.8 DSGVO eingeholt werden. Bei öffentlichen Veranstaltungen, z. B. Einschulungen, ist zudem vorab die grundsätzliche Einwilligung des Trägers einzuholen (Hausrecht).

(38) Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind.

✗ … bei Kamerasystemen, die den öffentlichen Bereich erfassen. Dazu der EuGH[33]:

*Soweit sich eine Videoüberwachung … auch nur teilweise auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre desjenigen gerichtet ist, der die Daten auf diese Weise verarbeitet, kann sie **nicht** als eine ausschließlich ‚persönliche oder familiäre' Tätigkeit … angesehen werden."*

➢ Rechtlich nicht abschließend geklärt sind Aufnahmen von Dashcams. Aus dem Beitrag des ADAC[34] zu diesem Thema ist zusammenfassend festzuhalten. Grundsätzlich sind permanente, anlasslose Aufzeichnung auch als „Hilfssheriff für Verkehrsverstöße" verboten. Aber, kurze anlassbezogene Aufnahmen (keine Daueraufnahme und/oder Dauerspeicherung LOOP-Funktion) von Unfällen können als Beweis verwertbar sein.

(b) „Tschüss TMG, welcome DDG"[35]

Wichtiger Hinweis zum Impressum auf der eigenen Seite im Netz bei den Pflichtangaben. Mit Inkrafttreten des neuen Digitale-Dienste-Gesetzes (DDG) am 14.05.2024 tritt gleichzeitig das Telemediengesetz (TMG) außer Kraft. Im Impressum ist der Hinweis auf die Pflichtangaben nunmehr auf die §§5,6 DDG zu beziehen und nicht mehr auf §5 TMG. Es mag unwahrscheinlich sein für viele, aber fällt es einer Aufsichtsbehörde auf, könnte es tiefergehende Rückfragen geben. Die Empfehlung ist einer kurzfristige Anpassung bei dem geringen Aufwand.

(c) Persönliche Daten im Handelsregister

Ein weiterer, interessanter Hinweis aus den Datenschutznotizen[36].

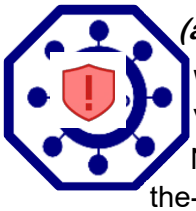
„Das Registergericht ist also verpflichtet, bei der Eintragung einer GmbH in das Handelsregister neben dem Familiennamen und Vornamen das Geburtsdatum und den Wohnort des Geschäftsführers dauerhaft einzutragen und die Einsichtnahme jedem zu Informationszwecken zu gestatten, ohne dass es der Darlegung eines berechtigten Interesses bedarf. …" (§§7,8 GmbHG, §24 HRV, §9 HGB Offenlegung)

Bedeutet, dass nach Art.6 Abs.1c DSGVO eine rechtliche Verpflichtung besteht und anhält, womit kein Recht auf Löschung (Art.17 DSGVO), Einschränkung (Art.18 DSGVO) und des Widerspruchs (Art.21 DSGVO) besteht.

„… und die Einsichtnahme jedem zu Informationszwecken zu gestatten, ohne dass es der Darlegung eines berechtigten Interesses bedarf. Hierbei stehen dem Registergericht weder ein Beurteilungsspielraum noch ein Ermessen zu, sodass es im Einzelfall entscheiden könnte, sondern diese Einsichtnahme ist stets zu gewähren."

So laut Datenschutznotizen ein Beschluss vom 23.01.2024 des Bundesgerichtshofs (BGH AZ.: II ZB 7/23).

(3) Zur Datensicherheit



(a) WLAN-Sicherheitslücke

Wie nicht nur heise-online[37] berichtet, besteht eine Sicherheitslücke in WLAN Netzwerken. Vereinfacht ausgedrückt, nie ein Netzwerkname (SSID) und Passwort für alle WLAN – Netzwerke einrichten. Dadurch kann sich ein Angreifer in den Netzwerkverkehr setzen (Man-in-the-Middle) und diesen verfälschen sowie Daten abgreifen. Vor allem sind die Standardeinstellung – immer - zu ändern. Jedes WLAN – Netzwerk sollte eine eigene Bezeichnung und ein separates Passwort erhalten. Für Administratoren zitiere ich hier aus dem, in der Fußnote verlinkten Artikel („ist einfacher"):

„Änderungen in den WLAN-Standards – Wi-Fi 7 bringe die Option des Beacon-Schutzes mit, der solche Angriffe vereitelt. Konkret können Netzwerk-Admins aber die Wiederbenutzung von Zugangsdaten zwischen SSIDs unterbinden. Enterprise-Netze sollten eigene CommonNames bei der Radius-Authentifizierung nutzen"

PS: Zu den selbst administrierten Netzwerken … ich könnte schwören (😉), dass zur Sicherheit schon immer die Standardeinstellungen zu ändern sind und jeder Zugang zu einem Netzwerk (z. B. in geschäftlich, privat und Gäste) zu trennen ist.

(4) Zu angrenzenden Themen

(a) Angriffe auf 2022 bereits behobene Schwachstelle???

Kann DAS sein? Wie „Security-Insider"[38] berichtet, greifen russische Hackergruppen derzeit eine Schwachstelle (CVE-2022-38028) im Windows-Druckerspooler mit Malware an. Microsoft hatte bereits *im Oktober 2022 ein Update zur Behebung* der Schwachstelle veröffentlicht. Der Angriff ist nach dem Artikel möglich, WEIL das Update auf vielen Rechnern nicht installiert und damit den Angreifern „Tür und Tor" öffnet. Die Bezeichnung „PC-Virus" ist nicht umsonst gewählt, weil notwendige Updates wie eine Schutzimpfung wirken. Es schützt nicht nur die eigenen Geräte, sondern auch vor der Verbreitung auf andere Geräte, sowie bei anderen Nutzern. Die Antwort auf die Frage also: „Verstehen kann ich es nicht wirklich, weil die Lücke ja geschlossen wurde bzw. ohne großen Aufwand geschlossen werden konnte und kann."

➔ 06@2024

(2) Zum Datenschutz

(a) „Datenschutzleitfaden für kleine Unternehmen der EDSA"[39]

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?"

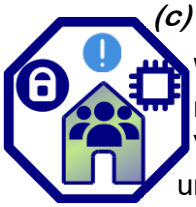
Die Erläuterungen mit Beispielen zum (bekannten 😉) Datenschutz sind sehr verständlich (auf Deutsch) beschrieben. Interessant sind auch die Hinweise zur Reaktion auf eine Datenschutzverletzung und die ggf. erforderliche Meldung an die zuständige Aufsichtsbehörde. Unter „Germany"[40] findet man auch gleich den Link zu seiner (den) zuständigen Aufsichtsbehörde(n) mit dem Meldeformular zum direkten Ausfüllen und Abschicken. Gut zu wissen, besser ist natürlich, wenn es nicht gebraucht wird! 😉

(b) „Schadenersatz! Was für ein Schaden?"[41]

Der Europäische Gerichtshof hat wieder mal entschieden[42], 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)[43].



(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[44]. 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 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 er-

halten. 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.[45] 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!

➔ 07@2024

(2) Zum Datenschutz

(a) Wofür jetzt „Standard-Datenschutz-Modell“

i) Ziel

Um die Verwirrung für Verantwortliche, Juristen, IT-Spezialisten und auch Datenschutzbeauftragte aus den gesetzlichen Anforderungen zu „entwirren“, haben die unabhängigen Aufsichtsbehörden des Bundes und Ländern ein Standard-Datenschutz-Modell entwickelt, um die praktischen, technischen und organisatorischen Maßnahmen in eine gemeinsame und verständliche Form und Sprache zu überführen (was sie auch international als Prüfmatrix nutzen wollen).

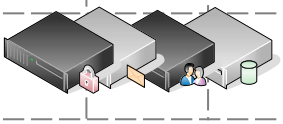
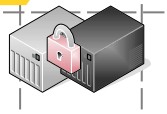
ii) Umsetzung

25 mehr oder weniger detailreiche gesetzliche Anforderungen nebst rechtlichen Ableitungen werden in übersichtliche 7 Gewährleistungsziele mit Erläuterung / Systematisierung, rechtlichen Anforderungen *und praktischen Ansätzen* überführt. Dabei sind die 3 Vertraulichkeit, Integrität und Verfügbarkeit nicht neu, sondern betreffen die Datensicherheit nach dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Den Datenschutz umfassen ergänzend Transparenz, Datenminimierung, Intervenierbarkeit und Nichtverkettung. Zuvor unter Nr. 1 befinden sich Links zum Datenschutzmodell der DSK, sowie einer Zusammenfassung.

iii) Übersicht (Prüfmatrix)

Ein weiteres Ziel ist die europaweite Vereinheitlichung der Datenschutzprüfung. Sehr anschaulich ist die entwickelte Prüfmatrix (von mir optisch etwas abgewandelt), oder: „Datenschutz ganz kurz“.

Was muss ich wissen und dokumentieren:

Verarbeitung ➔	Kollektion	Bereithaltung		Benutzung					Beseitigung
⬇Ebene	Sammeln	Aufbereiten	Aufbewahren	Bearbeiten	Benutzen	Bereitstellen	Verknüpfen	Einschränken	Beseitigen
Fachverfahren	Aktivität Aktivität	Aktivität				Aktivität		Aktivität	Aktivität
Fachanwendung	Anwendung			Anwendung	Anwendung			Anwendung	Anwendung
Infrastruktur									
	✔ Datenminimierung:	Zweck: angemessen, erheblich, notwendig							
	✔ Verfügbarkeit:	Verwendung: ordnungsgemäß, unverzüglich							
	✔ Integrität:	Datenschutz: fälschungssicher, verfügbar, unveränderbar							
	✔ Vertraulichkeit:	Zugriff und Nutzung nur durch Berechtigte							
	✔ Nichtverkettung:	Nur zweckgebundene Verwendung, Verknüpfung, Verkettung							
	✔ Transparenz:	Klarheit zu: Wer, was, womit, wofür, für wen!							
	✔ Intervenierbarkeit:	Recht auf Auskunft, Verwendung, Entscheidungshoheit							

✔ Mit dem Überblick im eigenen Interesse ist auch die Dokumentation recht einfach.

Neu in Version 3.1: Je nach Größenordnung der Organisation kann es sinnvoll sein, die Betriebsmittel (Anwendungen, Infrastruktur) zusätzlich zu gliedern nach unmittelbaren Betriebsmitteln (unverzichtbar, z.B. IT-Arbeitsplatz, E-Mail-System), mittelbaren Betriebsmitteln (Schutzfunktionen, z.B. Backup- und Schutzsysteme), spezifischen Betriebsmitteldaten (auch eigene Daten, z.B. Benutzerverwaltungsdaten und E-Mail-Adressen bei einem Videokonferenzsystem) oder unterschiedliche Anwendung nach Fachbereichen (z.B. IT, Personal, Vertrieb). Die Nachweispflichten sind immer auf Basis eines Gesamtverständnisses zu erstellen und mit Maßnahmen umzusetzen.

(b) Unordnung schützt (manchmal) vor den Anforderungen des Datenschutzes

Sehr schöner Beitrag im Jahresbericht der bayrischen Aufsichtsbehörde (Seite 39)[46]. Im Rahmen einer Beschwerde wurde moniert, dass in einem Café die Kundinnen und Kunden, die ihr Heißgetränk an der Theke bestellen, um Nennung ihres Vornamens gebeten werden. Grund hierfür war bzw. ist, die zubereiteten Getränke den an der Theke wartenden Kunden zuordnen zu können.

Für eine Datenschutzrelevanz sind 2 Kriterien erforderlich, die zumindest teilweise automatisierte Verarbeitung und die Verarbeitung in einem Dateisystem. Beides ist in diesem Fall nicht gegeben. Für den Cafébetreiber ist es allerdings wichtig, dass

„Soweit Namenszettel lediglich ungeordnet auf dem Tresen liegen und nach Namensaufruf entsorgt werden, fehlt es an dem Merkmal der Strukturiertheit einer Datensammlung.“

Die Entsorgung aber bitte im Reißwolf und nicht einfach im normalen Müll entsorgen. Alternativ bleibt dem Kunden, einen fiktiven Namen (anonymisiert) zu nennen, auch damit kann eine Bestellung zugeordnet werden.

(3) Zur Datensicherheit

(a) Anforderungen einer Cyberversicherung

Vorab wohl gemerkt, im Gegensatz zur Datensicherheit (Cyberversicherung) können erhöhte Risiken für Betroffene aus dem Datenschutz nicht durch eine Versicherung ausgeglichen bzw. minimiert werden, um eine Vorstellung bei der Aufsichtsbehörde zu verhindern.

Die bitkom e.V., als Vertreter von Software, IT-Services, Telekommunikation und Internetdienstanbietern hat einen Leitfaden zur Cybersicherung und -sicherheit aufgelegt [47]. Interessant fand ich die Mindestanforderung an kleine und mittelständische Unternehmen, damit die Versicherung im Schadensfall auch zahlt:

- Virenschutz mit automatischer Aktualisierung und Firewalls an allen Übergängen ins Netz.
- Regelmäßige Ransomware-sichere Backups (z.B. Offline, ext. Festplatte, Online unveränderbar).
- Regelmäßiger Patch-Management-Prozess sowie sicherer Betrieb bzw. das Ablösen von Altsystemen.
- Abgestuftes Rechtekonzept mit administrativen Zugängen ausschließlich für IT-Verantwortl.
- Absicherung von Fernzugriffen und Admin-Zugängen durch den Einsatz von Mehrfaktorauthentifizierung.
- Passwort-Richtlinien mit definierten Anforderungen an Länge und Stärke
- Datenschutzbeauftragter (intern oder extern) sowie verbindliche Datenschutzrichtlinien.
- Regelmäßige Sensibilisierung und Schulungen von Mitarbeitenden für IT-Sicherheit.

Für Industrieunternehmen kommen zusätzliche 10 Punkte hinzu. Mehr im verlinkten Leitfaden.

(4) Zu angrenzenden Themen

(a) BKA, Bundeslagebild 2023 Cybercrime [48]

Abbildung: BKA Bundeslagebild | Cybercrime 2023 (Seite 18)

Die positiven Nachrichten: Polizeiliche Maßnahmen schwächen zunehmend die globale Infrastruktur der Cybertäter. Die Aufklärungsquote ist bei den Cybercrime Delikten mit 32% leicht angestiegen und über 800 Unternehmen und Institutionen haben Ransomware-Angriffe zur Anzeige gebracht.

Die weniger positiven Nachrichten: Leicht rückläufigen Cyberstraftaten im Inland steht ein stärkerer Anstieg der Auslandstaten gegenüber. Die weltweiten Ransomware-Zahlungen steigen auf über USD 1 Mrd. DDoS Angriffe sind das „Mittel der Wahl“ hacktivistischer (politisch, ideologisch motivierte) Gruppierungen und einzelne Software-Schwachstellen wurden für massive Angriffskampagnen ausgenutzt.

➔ 08@2024

(2) Zum Datenschutz

(a) In 6 einfachen Schritten zum Verzeichnis der Verarbeitungstätigkeiten (1&2/6)

Einleitung:

Setzen wir mal voraus, dass nach §38 Abs.1 BDSG keine Datenschutzbeauftragter zu bestellen ist, weil weniger als 20 Mitarbeiter mit der Verarbeitung beschäftigt sind, keine geschäftsmäßige Datenübermittlung oder Sammlung zu Markt- und Meinungsforschung erfolgt und kein hohes Risiko für die Betroffenen besteht. Wenn doch, ist es eine gute Vorbereitung.

Aber *ein Verzeichnis der Verarbeitungstätigkeiten ist (99 %) immer zu führen*, allein schon aus dem einen Grund, dass nicht nur eine gelegentliche Verarbeitung erfolgt. Nach der Stellungnahme der Aufsichtsbehörden zu der Ausnahme zur Führung des Verzeichnisses nach Art.30 Abs.5 DSGVO: „*Wird sehr selten vorkommen!*“.

Um sich einen Überblick zu verschaffen, zunächst Schritt 1 und 2, was generell von Vorteil ist:

Schritt 1 (Sammeln/Speichern)

Welche Daten werden mit welcher Anwendung auf welcher Infrastruktur erhoben?

A.) Datenerhebung, -aufbereitung, -speicherung			
Lfd. Nr.	Aktivität Daten	Anwendung Applikation	Infrastruktur
1	<Name, Mailadresse – strukturiert in Listenform>	<Homepage, Mail-Account, Office-Suite>	<Webhoster, Cloud, PC>
2	<Name, Anschrift, Telefon – Kontaktdaten Vertrag>	<Homepage, Mail-Account - Vertragssoftware>	<Webhoster, Cloud, PC>

Einfach in Tabelle- oder Textdokument kopieren und sammeln.

Schritt 2 (Verwendung, Verknüpfung, Weitergabe)

Wie und womit werden die erhobenen Daten verwendet und an wen weitergegeben?

B.) Datenverwendung, -verknüpfung, -weitergabe			
Zu lfd. Nr. A	Aktivität Daten (-Kategorien)	Anwendung Applikation	Infrastruktur
1	<Newsletter>	<Mailsoftware>	<PC, Mailservice>
2	<Vertragsdokumentation und Kommunikation>	<Office-Suite, Abrechnungs-software, ext. Buchhaltung>	<PC, Mailservice, Verschlüsselung>

Einfach in Tabelle- oder Textdokument kopieren und sammeln.

Jetzt ist ein guter Monat Zeit zum Sammeln, bevor die nächsten Schritte anstehen 😉.

(b) Datenschutzrechte in den USA durchsetzen?

Kernaussage: „Der Datenschutz reist immer mit den Daten!“. Wenn Daten in ein Drittland (ex EU) übertragen werden, muss für diese Daten der gleiche Schutz wie in der EU gelten. Entweder werden nachweisbare, anwendbare Regelungen getroffen, oder die EU hat dies geprüft und für das Land einen sogenannten „Angemessenheitsbeschluss“ (eine Art EU-Prüfsiegel) dazu erlassen.

Im Juli 2023 wurde mit dem EU-US Data Privacy Framework (DPF) auch für die USA ein entsprechender Angemessenheitsbeschluss erlassen. Ein wichtiger Punkt für die Rechte der Betroffenen ist ein neues Beschwerdeverfahren mit dem laut BfDI:

> *Betroffene die Verarbeitung personenbezogener Daten durch US-Nachrichtendienste in den USA überprüfen lassen können. Neben diesem neuen Beschwerdemechanismus existieren weitere Beschwerdewege bei möglichen Verstößen gegen das DPF durch US-Organisationen/-Unternehmen.*[49]
>
> *Für Rechtsbehelfe gegenüber den US-Organisationen/-Unternehmen besteht für betroffene Personen unter anderem die Möglichkeit eine Beschwerde bei ihrer nationalen Datenschutzaufsichtsbehörde einzureichen, die von ihren Untersuchungs- und Abhilfebefugnissen nach der DSGVO Gebrauch machen kann.*

Für die Nutzung dieser Möglichkeit stellt das BfDI Informationen und ein Formular auf seiner Webseite zur Verfügung (Link in der Fußnote)[50].

(3) Zur Datensicherheit

(a) Windows 10 Updates endet 10/2025

Im Oktober 2025 endet die kostenlose Sicherheitsunterstützung für Win10 von Microsoft (!!!)[51]. Hauptoption ist ein Upgrade auf Windows 11, oder die Buchung von „Win10 Extended Security Updates“ oder bei Drittanbietern wie „0patch“ (Privat kostenfrei)[52].

(4) Zu angrenzenden Themen

(a) 10 Fallstricke beim Onlinebanking

PC-Welt hat in einem Artikel[53] die wesentlichen Fallstricke (und Schutzmaßnahmen) auch mit bildhafter Unterstützung zusammengetragen.

(1) ***Die Bank-Mail***: Ob ungewöhnliche oder unautorisierte Aktivitäten erkannt, das Limit überschritten, eine Fehlüberweisung erfolgte u.s.w. In allen Fällen wird man zur Gefahrenabwendung (Emotionen hervorrufen) gebeten, Kontakt über einen gefälschten Link aufzunehmen, über den dann Daten abgegriffen werden. Und die Texte sind immer perfekter. *Schutz:* Einfach nie einen Link aus einer Bank-Mail verwenden. Lieber das Bankportal direkt aufrufen und im Zweifel, insbesondere bei unerwarteten Mails, bei der Bank nachfragen.

(2) ***Bankmitarbeiter ruft an:*** Wie bei der Bank-Mail nur am Telefon wird versucht, Bankdaten zu bekommen. Zur Unterstreichung der Echtheit werden auch persönliche Daten genannt, die dem Internet / Social-Media entnommen sind (Recherche eigener Daten oft interessant). *Schutz:* Rückruf nur über bereits bekannte Telefonnummern vornehmen. Im Gespräch Telefonnummer erfragen, was der Polizei helfen kann.

(3) ***IBAN-Falle:*** Ein über dem Vergleich / Markt liegendes Angebot, z. B. Festgeld in Vergleichsportalen. Über den Link wird schnell (suggeriert) ein Konto eröffnet und man erhält eine IBAN zur Überweisung des Geldes. Die Bank und das Konto existieren meist im Ausland und der Betrüger hat hier Zugriff um über das Geld zu Verfügung. *Schutz:* Bei ungewöhnlich guten Angeboten nicht bekannter Quellen, Anbieter und Angebot über andere Kanäle prüfen und bei bekannten Anbieter den Direktkontakt suchen.

(4) ***Bessere Schufa-Bonität***: Es ist weniger ein Betrug, da Bonify ein völlig legaler Dienst per App ist, allerdings mit zweifelhaftem Wert. Die Bonität kann bei der Schufa jährlich einmal direkt angefordert werden. Um fehlerhafte Einträge muss man sich auch selbst kümmern. Aber mit den ausgelesenen Kontodaten der letzten 90 Tage werden einem Finanzprodukte angeboten. *Schutz:* Nicht empfehlenswert!

(5) ***Öffentliches WLAN***: Eine gute Sache, wenn Betrüger nicht auf die Idee gekommen wären „böse Zwillinge“ zu erstellen. *Schutz:* Wenn es denn sein muss, nur mit einem VPN-Dienst.

(6) ***Die Bank-SMS:*** Wie Bank-Mail (1), nur per SMS. *Schutz:* Siehe unter (1) Bank-Mail

(7) ***„Man-in-the-Browser“ Angriff:*** Über fehlende Sicherheitsupdates für den Browser oder nützliche Software / Erweiterungen verschafft sich der Betrüger Zugriff auf den Browser und setzt sich „heimlich“ zwischen die Kommunikation mit dem Onlinebanking. Greift dabei Daten ab, oder ändert im entscheidenden Augenblick unbemerkt die Kontonummer der Überweisung, oder leitet auf eine gefälschte Seite der Bank. *Schutz:* IMMER UP(TO)DATE für Browser und auch bei Erweiterungen auf Vertraulichkeit prüfen (weniger ist oft mehr).

(8) ***Session-Hijacking:*** Hier wartet der Betrüger mit Zugriff auf den Browser auf die Anmeldung im Onlinebanking und benutzt dann die „Session-ID“ für eigene Zweck im fremden Onlinebanking. *Schutz:* Wie unter (7).

(9) ***Unbegrenztes Limit:*** Bei unbegrenztem Überweisungslimit benötigt ein Betrüger nur eine gestohlene „Genehmigung“ (z.B. TAN), um das Konto incl. Kontolimit abzuräumen. *Schutz:* Nutzung des Angebots zur betraglichen Begrenzung von Einzeltransaktion.

(10) ***Veraltetes Betriebssystem:*** Ältere Betriebssysteme werden von den Anbietern nicht mehr mit Sicherheitsupdates unterstützt. Diese Lücken sind aber meist veröffentlicht und erleichtern Betrüger den Zugang, weil diese nicht mehr danach suchen müssen. *Schutz:* Ein aktuelles Betriebssystem mit Update-Support (ist nicht so teuer, lohnt sich aber).

➔ 09@2024

(2) Zum Datenschutz

(a) Verarbeitung öffentlich zugänglichen Daten

Auch für öffentlich zugängliche Daten gilt das Verbot mit Erlaubnisvorbehalt der DSGVO. Nach Art.14 DSGVO bestehen hier insbesondere die „üblichen“ Informationspflichten neben allen Rechten als Betroffener. Die Information nach Abs.1 und 2 hat nach Abs.3 innerhalb einer angemessenen Frist, jedoch spätestens innerhalb eines Monats zu erfolgen, sofort bei erster Kommunikation oder der ersten Offenlegung. Nach Abs.5 gelten Ausnahmen nur, wenn die betroffene Person bereits informiert ist, es unmöglich ist oder die Information einen unverhältnismäßig hohen Aufwand erfordert (z. B. wissenschaftliche und/oder historische Forschungszwecke).

Eine „Rechtsgrundlage“ der Verarbeitung besteht nur nach Art.6 Abs.1f, dem berechtigten Interesse des Verantwortlichen, sofern nicht die Schutzbedürftigkeit des Betroffenen überwiegt, d. h. es ist eine Abwägung vorzunehmen. Dazu lautet es im Erwägungsgrund 47 DSGVO u. a.

„… das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird.“

Dokumentieren bitte nicht vergessen!

(b) Austausch Kontaktdaten (u.a. Visitenkarten)

Wenn Kontaktdaten mittels Visitenkarte übergeben, oder digital zur Verfügung gestellt werden, gibt es nach Art.6 Abs.1 DSGVO folgende, einfache Gründe einer rechtmäßigen Verarbeitung (Abs.):

(1.a) Da heute die Führung eines Adressbuches nur noch in seltenen Fällen papierhaft erfolgt, kann eine Einwilligung zur Speicherung der Daten zwecks Kontaktaufnahme (NICHT Werbung, Newsletter u. ä.) angenommen werden. „Juristisch optimal“ ist natürlich im Nachgang eine Information der Verarbeitung zum Nachweis der Einwilligung an die Person zu senden. Das Risiko, einen Schaden auf genau dieser einen Kontaktdatenübergabe zurückzuführen dürfte selten bleiben.

(1.b) Die Verarbeitung ist für vorvertragliche Maßnahmen, z. B. die Übersendung oder Ausarbeitung eines Angebots erforderlich.

(1.c) Rechtliche Verpflichtung bei Übergabe von Geschenken (z. B. auf Messen).

(1.f) Im berechtigten Interesse des Verantwortlichen unter Abwägung der Schutzbedürftigkeit des Betroffenen. Der zuvor genannte Erwägungsgrund 47 DSGVO nennt beispielsweise auch das maßgebliche Bestehen einer Kundenbeziehung.

(c) In 6 einfachen Schritten zum Verzeichnis der Verarbeitungstätigkeiten (3&4/6)

Mit dem Schritt 1 (Sammeln/Speichern) und dem Schritt 2 (Verwendung, Verknüpfung, Weitergabe) ist ein sehr guter Überblick der zu verarbeitenden Daten geschaffen. Mit dem folgenden Schritt 3 (Einschränkung, Löschung) und dem Schritt 4 (Rechtsgrundlage) ist der wesentliche Teil der Dokumentation zum Datenschutz bereits abgedeckt.

Schritt 3 (Einschränkung, Löschung)

Wird die Datennutzung nach dem Zweck eingeschränkt und gelöscht?

C.) Datenverwendung Einschränkung und Löschung			
Zu lfd. Nr. A	Aktivität Daten	Anwendung Applikation	Infrastruktur
1	<Bei Widerruf, Abbestellung>	<Mailsoftware>	<PC, Mailservice>
2	<Einschränkung bei Vertragsende, Löschung nach GoBD>	<Office-Suite, Abrechnungssoftware, Buchhaltung>	<PC, Mailservice>

Einfach in Tabelle- oder Textdokument kopieren und sammeln 😉.

Schritt 4 (Rechtsgrundlage)
Ist nach Art.6 DSGVO eine der folgenden Bedingungen für die Verarbeitung erfüllt?

D.) Rechtsmäßigkeit der Verarbeitung						
Zu lfd. Nr. A	a) Einwilligung zur Verarbeitung	b) Vertragserfüllung oder die Anbahnung*	c) Rechtliche Verpflichtung	d) Wichtige Interessen der Betroffenen	e) Im öffentlichen Interesse vorgeschrieben	f) Berechtigtes Interesse Verantwortliche
1	X, bestätigt.					
2		X1	X2 nach GoBD			

**) Nach Art.6 Abs.1b DSGVO ist die Datenverarbeitung zu Zwecken der Anbahnung von Vertragsverhältnissen erlaubt (vorvertragliche Maßnahmen). „Hierunter könnte man im Einzelfall auch schon die Übergabe von Visitenkarten oder andere Übermittlung von Kontaktdaten, Absenderangaben subsumieren". Für Werbung oder Newsletter u. ä. ist eine separate Einwilligung einzuholen!.*

Einfach in Tabelle- oder Textdokument kopieren und sammeln 😉.

(3) Zur Datensicherheit

(a) Gefahr durch Schadsoftware nicht bekannt?

Aus einer gemeinsamen Befragung der polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist der Cybersicherheitsmonitor 2024 mit dem Fokusthema: „Smarthome"[54] erstellt worden. Erschreckende Ergebnisse: „***Die Gefahr durch Schadsoftware ist vielen Nutzern nicht bewusst***"

- *Weniger als die Hälfte der Befragten (42 %) ist sich bewusst, dass Smarthome-Geräte mit Schadsoftware infiziert werden können.*
- *Nur etwa vier von zehn Nutzern kennen das Risiko, dass durch kompromittierte Geräte persönliche Daten ausgespäht und missbräuchlich verwendet werden können.*
- *Fast jeder Dritte gibt an, keines der typischen Smarthome-Risiken zu kennen.*

Wenn nicht die Polizei und das BSI die Befragung durchgeführt hätten, hätte ich es nicht geglaubt. Deshalb kommt der regelmäßigen Sensibilisierung aller Beteiligten in der Organisation unverändert ein hoher Stellenwert zu. Der Schutz vor Cyberkriminellen ist im Interesse des Mitarbeiters und des Unternehmens.

(b) Und die Gefahr wächst!

Nach einem Bericht des Spiegels zu Zahlen der Versicherungsgesellschaften[55] nehmen die Schäden durch Cyberangriffe drastisch zu. Nur den Versicherungen wurde im letzten Jahr 4.000 Angriffe (+19 %) mit einem durchschnittlichen Schaden von € 45.000 (+8 %) gemeldet. Nach dem GKV-Hauptgeschäftsführer (Jörg Asmussen) wird es insbesondere im Mittelstand mit dem Versicherungsschutz schwer, wenn dort die IT-Sicherheitslücken weiter „klaffen".

(4) Zu angrenzenden Themen

(a) Positiv aufgefallen

✔ Das Bundesamt für Sicherheit in der Informationstechnik (BSI) vergibt für Anwendungen ein IT-Sicherheitskennzeichen, d. h. die Hersteller geben eine detaillierte Erklärung (Verpflichtung) zur Sicherheit ihrer Anwendungen ab, die vom BSI geprüft und für gut befunden werden muss, um dieses Kennzeichen zu erhalten. Erhalten haben es u. a.:

- IT-Sicherheitskennzeichen für **Zoom Workplace Basic**[56]
- IT-Sicherheitskennzeichen für **Zoom Workplace Pro**[57]

✔ Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Informationen über ein Projekt zur Mitarbeit veröffentlicht, dass die Sicherheit in **LibreOffice** erhöht. Das durch das BSI initiierte Projekt startete im September 2023 und wurde von zwei unabhängigen Dienstleistern bearbeitet. In einem ersten Schritt wurden die Entwicklungsarbeiten in LibreOffice von der Firma allotropia software GmbH geleistet. Anschließend wurde ein Audit der Sicherheitseigenschaften von der OpenSource Security GmbH durchgeführt.[58]

➔ 10@2024

(2) Zum Datenschutz &

(3) Zur Datensicherheit

(a) Datensicherheit zum Datenschutz

Wie schon in Verordnung und Gesetz geregelt, muss nicht jeder, vom (Solo-) Selbständigen über KMUs bis zu „Internetgiganten“, alle weltweit möglichen Schutzmaßnahmen und Sicherheitsanwendung einsetzen. Zur „Sicherheit der Verarbeitung“ führt Art.32 DSGVO aus:

„(1) Unter Berücksichtigung des Stands der Technik,“

- Die Technik sollte schon dem aktuellen Niveau entsprechen.

„… der Implementierungskosten“

- Die Kosten sollen sich in einem angemessenen Rahmen zu den verarbeiteten Daten bewegen und müssen nicht überborden.

„... und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung“

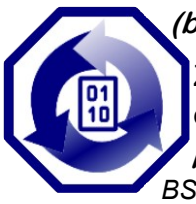
- Je größer Art, Umfang und Zweck, zum Beispiel große Mengen an Daten verteilt über eigene, Rechenzentren, Dienstleister, Cloud und verteilt über Landesgrenzen erfordern höhere Schutzmaßnahmen und damit Kosten, als ein eigener, einzelner Client bzw. Rechenzentrum.

„... sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“

- Hiermit ist der besondere Schutz für besondere Kategorien personenbezogener Daten nach Art.9 DSGVO gemeint. Daneben sind auch beispielhaft Daten zum Identitätsdiebstahl oder dem Kontozugriff gemeint oder der Verlust wichtiger Daten für die betroffene Person. Alle Daten, die ein hohes Schadensrisiko bei Verlust für den betroffenen bedeuten. Das kann dann auch höhere Aufwandskosten zum Schutz bedeuten.

... treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; ...

- Zu den organisatorischen Maßnahmen gehört der räumliche Schutz der Verarbeitungstechniken, z. B. Zutrittsberechtigungen, Schutz vor Feuer, Wasser und technischem Ausfall. Die Mitarbeiter sind zur Einhaltung zu verpflichten (Datenschutzrichtlinie), zu informieren (Merkblatt & Information) und regelmäßig über die Schutzmaßnahmen und Gefahren mindestens durch jährliche Schulungen zu sensibilisieren.
- Zu den technischen Maßnahmen gehören eine ausreichende Belastbarkeit der Systeme zur Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit, sowie Wiederherstellung nach einem Zwischenfall. Außerdem sollte eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit erfolgen.



(b) Geeignete technische Maßnahmen zur Datensicherheit?

Zur Auswahl von geeigneten technischen Maßnahmen stellt das Bundesamt für Sicherheit in der Informationstechnik verschiedene Stufen zur Cybersicherheit zur Verfügung.

i) Leichter Einstieg (KMUs)[59]

BSI: „In Zeiten der Digitalisierung kommen auch kleine und mittlere Unternehmen nicht umher, sich in Sachen Cyber-Sicherheit weiterzuentwickeln.“ (Basiselemente)

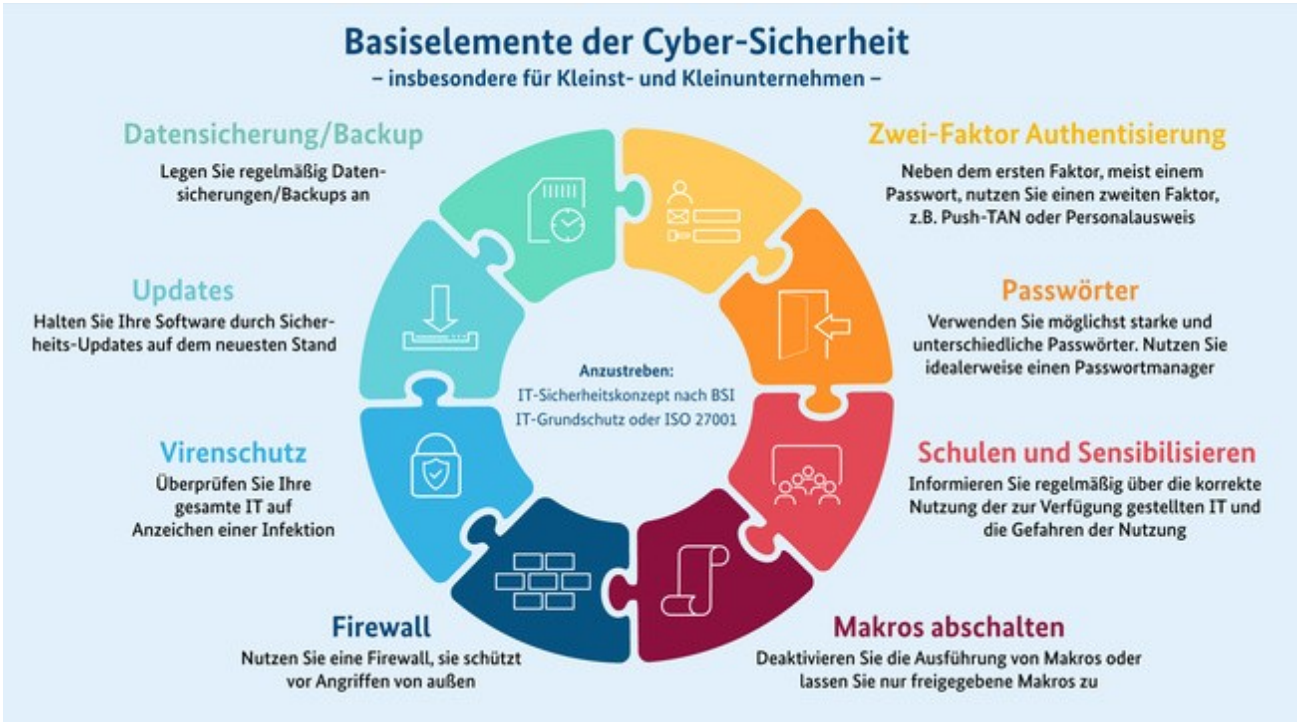


Schaubild: Quelle: Bundesamt für Sicherheit in der Informationstechnik

Eine zusammenfassende Erläuterung der Basiselemente zum Einstieg in die Cyber-Sicherheit für kleine Unternehmen, Selbstständige und Interessierte stelle ich hier kurz auf 6 Seiten zur Verfügung: https://volkerschroer.de/DSGVO/BSI.Einstieg.Cybersicherheit.pdf

ii) BSI IT-Grundschutz (mit Branchenprofilen)

Das BSI hat über 25 Jahre einen oder den IT-Grundschutz[60] entwickelt und entwickelt diesen nach dem Stand der Technik weiter. Der IT-Grundschutz ist praxisnahe im modularen Bausteinsystem zu allen relevanten Themen aufgebaut und bietet konkrete Sicherheitsanforderungen nach entsprechenden Branchenprofilen. Aus einer Schulung zum Basiswissen BS / IT-Grundschutz habe ich hier eine kurze und knappe Zusammenfassung (Management-Information) zusammengestellt: https://volkerschroer.de/DSGVO/BSI.Basiswissen.IT-Grundschutz.pdf.

(c) 5 & 6 von 6 einfachen Schritten zum Verzeichnis der Verarbeitungstätigkeiten

i) Schritt 5 (Datensicherheit)

Sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Umstände (Umfang, Zweck, Betroffenenrisiken) geeignete technische und organisatorische Maßnahmen für ein angemessenes Schutzniveau gewährleistet (Datensicherheit)?

E.) Sicherung der Verfügbarkeit, Vertraulichkeit und Integrität	
je-weils	O = organisatorische Maßnahmen | T = technische Maßnahmen | I = Betroffene informiert
T.)	<Zentral gesteuerte Firewall und Virenscanner>
O.)	<Unternehmensweite Mitarbeiterrichtlinie zum Datenschutz und Datensicherheit>

Einfach in Tabelle- oder Textdokument kopieren und sammeln 😉.

ii) Schritt 6 (Verzeichnis zusammenstellen)

Formvorschriften für das Verzeichnis der Verarbeitungstätigkeiten nach Art.30 DSGVO und BDSG.

„Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.“ (ErwGr: (82) DSGVO)

Dazu ist eine:

➔ Dokumentation in schriftlichem oder auch in elektronischem, unterzeichnetem Format (Abs.3), mit Name und Kontaktdaten von Verantwortlichen, sowie ggf. Datenschutzbeauftragten (Abs.1a).

➔ Diese Daten sind mit Kopien von Schritt 1 bis 5 (A bis E) zu ergänzen, da bereits enthalten:

- ✔ Beschreibung von Zweck und Kategorien der Personen & Daten der Verarbeitung (Abs.1b,c).
- ✔ Wer erhält Daten (interne & externe Empfänger in Europa, Drittland, intern. Organisation)
- ✔ und ist die Einhaltung der Datenschutzvorschriften (ex EU) gewährleistet. (Abs.1d,e i.V.m.Art.49).
- ✔ Wenn möglich, vorgesehene Löschfristen und eine allgemeine Beschreibung der technisch – organisatorischen Schutzmaßnahmen nach Verhältnismäßigkeit und dem aktuellen Stand der Technik (Abs.1f,g i.V.m. Art.32).
- ✔ Die gleichen Angaben sind für Auftragsverarbeiter (Dienstleister) zu dokumentieren (Abs.2).
- ✔ Rechtsgrundlage der Verarbeitung (§70 Abs.1 Nr.7 BDSG).
- ✔ Alternativ zu Löschfristen die Überprüfungstermine zur Notwendigkeit (Abs. 1 Nr.8).

Dokumentation Datenschutz und -sicherheit,

➢ *Sinnvolle Ergänzungen sind* Datum der Erstellung und Änderung, Art und Transparenz von Einwilligungen, Aufstellung der Auftragsverarbeiter, Sensibilisierung der Mitarbeiter, Einhaltung von Betroffenenrechten, den Umgang mit Meldepflichten, Schutzverletzung und von Risikoeinschätzungen.

➢ „Schön schreiben“ kann man es natürlich auch (z. B. Link zu Erläuterung und Muster).

➔ 11@2024

(2) Zum Datenschutz

(a) Zusammenfassung: „Einfach ein Verzeichnis der Verarbeitungstätigkeiten erstellen“

Natürlich gibt es auch eine Zusammenfassung zu den 6 einfachen Schritten zur Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten nach Art.30 DSGVO in Verbindung mit § 70 BDSG hier: https://volkerschroer.de/DSGVO/Verzeichnis.Verarbeitungstaetigkeiten.schlank.pdf mit Erläuterung der Anforderungen, Musteransicht und einer kleinen FAQ zu oft gestellten Fragen.

(b) App-Prüfung einer Aufsichtsbehörde

Aus dem 13. Tätigkeitsbericht des Bayrischen Landesamts für Datenschutzaufsicht (BayLDA)[61] zur Prüfung von Apps mit Fokussierung auf einwilligungspflichtige Dienste.

„Oftmals erfolgen bereits einwilligungspflichtige Vorgänge wie beispielsweise das Auslesen von IDs aus dem Smartphone direkt nach Installation der App, ohne dass Nutzende mit einem Einwilligungsbanner interagieren und somit ohne, dass über eine rechtswirksame Einwilligung entschieden werden konnte. Einige App-Betreiber verzichteten sogar komplett auf Einwilligungsbanner und beriefen sich auf Geräteeinstellungen, die das App-Tracking unterbinden könnten. Dies war vor allem bei iOS-Geräten häufiger der Fall, da Apple mit der Funktion „App Tracking Transparency“ - kurz ATT - die Möglichkeit bietet, App-Tracking zu erlauben oder zu versagen.“ (14.1 Seite 62 / Ähnliches geht auch mit der Werbe-ID bei Android[62])

Damit ist die Informationspflicht und der Inhalt nach Art.13 DSGVO nicht eingehalten.

Häufig kamen Dienste wie Google Analytics und Facebook Pixel direkt beim Starten der App zum Einsatz, ohne dass die hierfür notwendige Einwilligung eingeholt wurde.

Dabei spielt es keine Rolle, ob personenbezogene Daten (wie IP-Adresse) verarbeitet wurden, oder die Berufung auf ein berechtigtes Interesse nach Art.6 Abs.1f DSGVO, denn in diesem Fall zieht das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) mit § 25.

Dieser schützt bereits die Integrität des Gerätes an sich und fordert daher regelmäßig eine Einwilligung für das Speichern oder Auslesen von Informationen wie beispielsweise Geräte-IDs.

Mir stellt sich die Frage: „Wo ist das Problem, offen mit der Datennutzung umzugehen?“. Denn:

Wird eine Einwilligung vom Webseiten oder dem App-Betreiber nicht eingeholt, trotz mittlerweile eindeutiger Rechtslage, prüfen wir die Verhängung eines Bußgelds.

(c) Kuriosität aus dem Bericht der BayLDA

Bei vielen Verstößen fehlte laut Bericht bereits die Rechtsgrundlage nach Art.6 DSGVO, so auch bei einer Videoüberwachung (Video mit Ton) durch eine Wildkamera, die in einem

Gebüsch an einem FKK-Badebereich eines Badesees versteckt angebracht wurde. Die zuständige Staatsanwaltschaft stellte das Ermittlungsverfahren ein, sodass wegen dieses Sachverhalts ein Bußgeld nach der DSGVO verhängt werden konnte. (18.1 Seite 82)

(d) Datenschutzbeauftragter erst ab 50 statt 20 Personen Pflicht?

VORAB: Alle Regeln des Datenschutzes sind durch den Verantwortlichen einzuhalten, ob er verpflichtet ist, einen Datenschutzbeauftragten (intern oder extern) zu benennen oder nicht!

Hier geht es um die Erleichterung zu Art.37 DSGVO der Benennung eines Datenschutzbeauftragten (intern / extern) in Verbindung mit § 38 BDSG Datenschutzbeauftragter nicht öffentliche Stellen, dort lautet es:

„… benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.“

Aber, es geht weiter mit:

Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 679/2016 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

Und, diese Änderung ist zur Bürokratieerleichterung im Haushalt eingeflossen, und dieser ist noch nicht beschlossen. Schaut man sich die Positivliste der Datenschutzkonferenz[63] mit Pflicht zur Erstellung einer Datenschutz - Folgenabschätzung an, ist die Befreiung von der Benennung recht schnell hinfällig. Allein die Abwägung zum Rechtsgrund des berechtigten Interesses (Art.6 Abs.1f DSGVO) kann schnell zu einem Erfordernis führen.

Meinung: Der § 38 BDSG ist gut, aber ob jetzt 20 oder 50 macht keinen zu großen Unterschied, und eine Entscheidung wird aller Voraussicht nach erst nach den nächsten Bundestagswahlen fallen.

(3) Zur Datensicherheit

(a) Studie „Führungskräfte im Fadenkreuz“

GetApp (Vergleichsplattform für Unternehmenssoftware) bietet „objektive, unabhängige Studien“, so die Webseite. Ziel der Studie zu „Cyberangriffe auf deutsche Unternehmen & Führungskräfte“[64] im Mai 2024 unter 2.648 Befragten in Europa, USA, Kanada, Brasilien und Mexiko in Unternehmen die Sicherheitssoftware verwenden, ob sie an Cybersicherheitsmaßnahmen beteiligt sind oder diese kennen. Natürlich werden hier auch Tools & Tipps angeboten, was hier nicht der Fokus ist, sondern die Ergebnisse, um aus Fehlern zu lernen, da gerade Führungskräfte im Fokus von Cyberkriminellen stehen.

- Zwei von drei Führungskräften waren in den letzten 18 Monaten Opfer einer Cyberattacke.
- Führungskräfte fallen immer noch auf Phishing-Angriffe rein. Diese sind die häufigste Art mit einem Anteil von 56 % der Befragten, gefolgt von Mailware-Angriffen 49 % und jeweils 1/3 entfällt auf Identitätsdiebstahl, Ransomware und Deepfake-Angriffe.
- Handlung von Führungskräften, die zu einem Cyberangriff führten:
  41 % Download von Dateien aus nicht vertrauenswürdigen Quellen
  41 % Nutzung schwacher Passwörter
  34 % Ignorieren von Schulungen zur Cybersicherheit & die Wichtigkeit von Verschlüsselung
  33 % Umgehung von Sicherheitsrichtlinien und mangelnde, aktuelle Updates
  24 % Weitergabe sensibler Informationen über unsichere Kanäle.
- Die daraus folgenden Arten von Identitätsbetrug entfielen fast jeweils zur Hälfte auf Dokumentenbetrug, Kompromittierung von Geschäftskorrespondenz wie E-Mails, Datenlecks, betrügerische Finanztransaktionen und kompromittierte Anmeldeinformationen.

Fazit: Eine regelmäßige Erinnerung auch in Form von Schulungen ist unverändert wichtig und für alle Parteien interessant, da Cyberkriminelle keinen Unterschied zwischen privatem und geschäftlichem Opfer machen.

(4) Zu angrenzenden Themen

(a) Datenschutzerklärung – verständlich ☺

Alles, was man zu gutem Datenschutz wissen sollte endlich mal verständlich in einem kurzen Video *(Video, nicht der Text)* hier: https://kids.lego.com/de-de/legal/privacy-policy viel Spaß.

(b) Kann mein Chef meine ChatGPT-Anfragen lesen?

Ein interessanter Artikel von moz://a (Mozilla Foundatin / Firefox, Thunderbird)[65]. Ok, ganz so einfach ist es nicht! Für alle, die sich fragen, ob ihr Chef ihre ChatGPT-Anfragen lesen kann, lautet die Antwort: Es ist kompliziert. Ihr Chef kann Ihre ChatGPT-Protokolle nicht direkt einsehen, aber die App ist auch nicht gerade eine Bärenfalle. Ein Admin kann nicht erfolgreich ChatGPT fragen: „Zeig mir alles, was Xavier gesucht hat.“ Nur, ChatGPT hat eine seltsame Angewohnheit, Informationen preiszugeben, die es anderswo gelernt hat. Mit der richtigen Frage kann ChatGPT Informationen ans Licht bringen, die andere für privat oder vergessen hielten. Zusätzlich zu den richtigen Fragen könnte es möglich sein, einen Drittanbieterdienst zu nutzen, um die Aktivitäten der Mitarbeiter auf ChatGPT zu überprüfen. Diese Tools sind nicht in ChatGPT integriert, aber es ist durchaus machbar, die Eingaben anderer Mitarbeiter über ein Drittanbieter-Tool zu erfahren.

➔ 12@2024

(2) Zum Datenschutz

(a) Outlook (New), alte und neue Bedenken

Unzureichender Datenschutzinformation der Nutzer bereiten der Aufsicht ja schon länger Bedenken zu Microsoft Office. Dazu berichtete die Landesbeauftragte für Datenschutz und Informationssicherheit LDI-NRW bereits Ende letzten Jahres[66].

„Vollständiger Postfachzugriff bei trüber Transparenz
*Während der Einrichtung der neuen Outlook-Version werden Nutzer*innen lediglich darauf hingewiesen, dass eine Synchronisation mit der Cloud erfolgt. Dagegen wird nach jetzigem Kenntnisstand keine wirksame Einwilligung nach Art. 6 Unterabsatz 1 Satz 1 Buchstabe a DS-GVO eingeholt. Insbesondere informiert Microsoft nicht darüber, dass die Zugangsdaten ebenfalls in die Cloud übermittelt werden.*
Die LDI NRW weist darauf hin, dass bei der Nutzung der neuen Version Microsoft ein vollständiger Zugriff auf das Postfach ermöglicht wird. Die geführte Korrespondenz inklusive möglicher Anhänge werden dabei in der Cloud gespeichert und von Microsoft verarbeitet. Es bleibt unklar, zu welchen konkreten Zwecken die Verarbeitung dieser Daten erfolgt.
Die neue Outlook-Version gehört zu den Microsoft365-Diensten. Auch bei einer früheren Prüfung der Microsoft365-Dienste hatte die Datenschutzkonferenz die mangelnde Transparenz der Datenverarbeitung beanstandet sowie die resultierende Schwierigkeit für Verantwortliche, ihrer Rechenschaftspflicht nachzukommen.“

i) Automatische Umstellung: ☹

Heise online berichtet, dass Microsoft alle Business-Kunden zum 6. Januar 2025 automatisch auf das neue Outlook umstellen wird.[67]

ii) Datenschutz: ☹

Es fehlt die Rechtsgrundlage (keine Zustimmung, keine vertraglichen Gründe, keine gesetzlichen Erfordernisse und kein berechtigtes Interesse) und es bleibt unklar, wozu die vollständigen Daten jedes einzelnen Postfachs in Kopie in der Cloud vorgehalten und analysiert werden

iii) Datensicherheit: ☹

Sofern korrekt werden z. B. auch Zugangsdaten in der Cloud gespeichert, womit ein Zugriff auf das Postfach und anderes möglich ist (um nur eins der Themen zu nennen),

iv) DATEV: ☹

In einem Blogbeitrag im „DATEV Hilfe-Center“[68] lautet es:

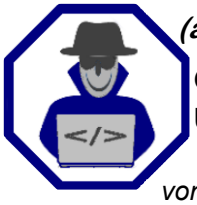
„Ein Einsatz des neuen Outlook im Zusammenhang mit DATEV-Programmen wird nicht unterstützt.

Microsoft Outlook new bietet keine COM-Schnittstelle an, die für die Nutzung mit DATEV-Programmen zwingend erforderlich ist. Entsprechende Funktionen zur Erstellung, Bearbeitung und/oder der Ablage von E-Mails, z. B. in DATEV DMS, Kanzlei-Rechnungswesen, DATEV Anwalt etc., werden bei Einsatz von Microsoft Outlook new nicht unterstützt.“

Dort werden nicht nur auf die Gründe und die Zeitpläne eingegangen, sondern auch die Maßnahmen vorgeschlagen, um die automatische Umstellung auf „Outlook (new)“ zu unterbinden.

Wer „tiefer“ sucht, könnte noch auf andere Punkten stoßen.

(3) Zur Datensicherheit



(a) Fokus: Cyberangriffe auf Führungskräfte

GetApp (Empfehlung von Software) hat eine Studie zum Thema „Cyberangriffe auf deutsche Unternehmen und Führungskräfte“ veröffentlicht[69].

„Führungskräfte stehen im Fadenkreuz von Cyberkriminellen, und ihr Schutz ist für das Unternehmen von entscheidender Bedeutung. Unsere Studie zeigt, welchen Risiken Führungskräfte ausgesetzt sind und mit welchen Tipps und Tools Unternehmen ihre Cybersicherheit verbessern können.“

Einige Highlights aus der Studie:

- ✗ Ca. 2/3 der Führungskräfte sind in den letzten 18 Monaten Ziel eines Angriffs gewesen
- ✗ Ca. 2/3 der Unternehmen sind schon einmal Ziel von Angriffen gewesen.
- ✗ Ca. 1/3 der Führungskräfte ignorierten Sicherheitsschulungen.
- ✗ Phishing-Angriffe sind immer noch das größte Cybersicherheits-Risiko.

Handlungen von Führungskräften, die zu Cyberangriffen führten waren:

- Download von Dateien aus nicht vertrauenswürdigen Quellen.
- Schwache Passwörter.
- Ignorierung von Sicherheitsschulungen.
- Ignorierung der Bedeutung von Datenverschlüsselung.

Die Lösung scheint offensichtlich einfach: „Zeit für Schulung auch für Führungskräfte“. Mehr Ansätze sind natürlich auch in der Studie aufgeführt.

(4) Zu angrenzenden Themen

(a) Wie geht es jetzt mit der E-Rechnung

Die Frage ist (nicht nur mir und mit mir) in letzter Zeit oft gestellt und diskutiert worden, weil „ab 01.01.2025 Pflicht?“. Das Bundesministerium der Finanzen schreibt in der Einleitung zu den FAQs[70] (kryptisch):

Mit dem Wachstumschancengesetz sind die Regelungen zur Ausstellung von Rechnungen nach § 14 UStG für nach dem 31. Dezember 2024 ausgeführte Umsätze neu gefasst worden. Ab dem 1. Januar 2025 ist bei Umsätzen zwischen inländischen Unternehmern regelmäßig eine elektronische Rechnung (E-Rechnung) zu verwenden. Bei der Einführung dieser obligatorischen (verpflichtenden) E-Rechnung gelten Übergangsregelungen. Insbesondere private Endverbraucher sind von diesen Regelungen nicht betroffen.

i) Ausnahmen:

Ausgenommen von der Pflicht zu einer E-Rechnung sind Kleinbeträge (< € 250,00), Fahrausweise, Leistung von Kleinunternehmer (Umsatzsteuerwahlrecht), Leistungen an Endverbraucher, im Zusammenhang mit einem Grundstück und Vereine, sofern sie nicht unternehmerische Tätigkeiten ausüben.

ii) Übergangsregelungen

- ✔ Bis Ende 2026 können sich Rechnungsaussteller für eine Alternative zur E-Rechnung (Papier, oder mit Zustimmung des Rechnungsempfängers auch andere Formate) entscheiden.
- ✔ Ab 01.01.2025 besteht also nur eine Pflicht, E-Rechnung empfangen zu können.
- ✔ Die Übergangsregelung verlängert sich noch mal bis Ende 2027, bei Nutzung des Formats „EDI“ und bei einem Vorjahresumsatz des Rechnungsstellers von < € 800.000,00.

iii) Datenschutz

Steuerberater sind nach ihren Berufspflichten weisungsfrei und ihren Mandanten verantwortlich (§ 11 Steuerberatungsgesetz), d. h. in gemeinsamer Verantwortung, sodass ein Auftragsverarbeitungsvertrag nicht erforderlich ist.

Bei allen anderen „Service- und Softwareanbietern“ ist eine Auftragsverarbeitungsvertrag zwingend und wird auch i. d. R. mit einem Abschluss gleich angeboten und ist zu dokumentieren. Beispiele dafür sind „lexoffice“[71], „sevdesk“[72], buhl/WISO[73] und jeder Kunde der DATEV[74] als berufsständisches Softwarehouse und IT-Dienstleister.

iv) Datensicherheit

Sicherlich gibt es viele, auch kostenfreie Anbieter mit einer Abwicklung in der Cloud und auch dem Versprechen, die Daten nach Gebrauch sofort zu löschen. Das reicht aber nicht. Da der Übertragungsweg zu sichern ist und die Daten mit Übertragung offengelegt sind. Es gilt ja der Grundsatz in der DSGVO: „Datenschutz reist immer mit den Daten!“.

(b) KI-Oma treibt Betrüger in den Wahnsinn[75]

Die alte Dame (KI-Oma) „DAISY“ verwickelt Kriminelle in teils stundenlange Gespräche. Von O2 in Großbritannien vorgestellt, schaltet die „DAISY“ sich bei Nutzung spezieller Telefonnummern der Kriminellen ein. 👍

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“
23 Quelle: Deutsche Gesellschaft für Datenschutz: „Wie kann diese Rechtsgrundlage zur Rechtfertigung für Verarbeitung...“
24 Quelle: WDR-Nachrichten: „Immer mehr Bürger zeigen Falschparker an“
25 Quelle: ADAC: „Urteil: Darf man Falschparker fotografieren“
26 Quelle: BAYERN.RECHT: „VG Ansbach, Urteil v. 02.11.2022 – AN 14 K 22.00468“
27 Quelle: LibreOffice: „German state moving 30,000 PCs to LibreOffice“
28 Quelle: Landesreg. Schleswig-Holstein: „Einstieg in den Umstieg: Schleswig-Holstein setzt auf einen digital souveränen“
29 Quelle: Der Westen (WAZ): „DHL macht Schluss bei Live-Verfolgung der Pakete“
30 Quelle: BSI: „Linux-betriebsystem BSI warnt vor gravierender Sicherheitslücke“
31 Quelle: Commerzbank: „EuGH schränkt Einfluss des Schufa-Scores ein“
32 Quelle: InfoCuria: „EuGH C-345/17 vom 14.02.2019“
33 Quelle: InfoCuria: „EuGH C-212/13 vom 11.12.2014“
34 Quelle: ADAC: „Dashcams. Was erlaubt ist und was nicht“
35 Quelle: Datenschutznotizen: „Tschüss TMG, welcome DDG“
36 Quelle: Datenschutznotizen: „Art. 17 Abs. 1 DSGVO gilt nicht für GmbH-Geschäftsführer“
37 Quelle: heise-online: „WLAN-Attacke: SSID-Verwechslungs-Angriff macht Nutzer verwundbar“
38 Quelle: security-insider.de: „Cyberkriminelle greifen Druckerspooler in Windows an, viele Rechner angreifbar“
39 Link: EDSA Datenschutzleitfaden für kleine Unternehmen https://www.edpb.europa.eu/sme-data-protection-guide/home_de
40 Link: Meldeformulare der Aufsichtsbehörden: https://www.edpb.europa.eu/notify-data-breach_de
41 Quelle: Legal Tribune Online, 20.06.2024 EuGH zur DSGVO: Datenklau als immaterieller Schaden?
42 Quelle: InfoCuria: „EuGH-Urteil C-182/22 und C-189/22 Anspruch auf Ersatz des Schadens nach der DSGVO.“
43 Quelle: CMS law tax future: „DSGVO-Schadenersatz Übersicht, aktuelle Urteile und laufende Entwicklung“
44 Quelle: dejure.org: „Volltextveröffentlichungen BGH, 06.02.2024 – VI ZR 15/23“
45 Quelle: chip.de: „Versteckt in unscheinbaren Popups: Forscher warnen vor gefährlicher Sicherheitslücke“
46 Quelle: 13. Tätigkeitsbericht BayLDA: „Kaffeebestellung mit Namensaufruf“
47 Quelle: bitkom e.V.: „Leitfaden Cyberversicherung und -sicherheit“
48 Quelle: BKA: „Bundeslagebild 2023 Cybercrime“
49 Pressemitteilung des Bundesbeauftragten für Datenschutz und Informationsfreiheit: „Kurzmeldung“
50 BfDI: „Beschwerdeverfahren zum EU-US DPF“
51 Microsoft: „Supportzeiträume“;
52 0patch: Startseite (nur Beispiel, keine Werbung u/o gegen Entgelt u.ä.)
53 PC-Welt: „Achtung: Zehn Fallen beim Onlinebanking“
54 Quelle: ProPK & BSI: „Cybersicherheitsmonitor 2024 mit dem Fokusthema: „Smarthome““
55 Quelle: Speigel Netzwelt: „Schäden durch Cyberangriffe nehmen drastisch zu“
56 Quelle: BSI: „IT-Sicherheitskennzeichen für Zoom Workplace Basic“
57 Quelle: BSI: „IT-Sicherheitskennzeichen für Zoom Workplace Pro“
58 Quelle: BSI: „BSI erhöht Sicherheit in LibreOffice“; und Details zu „Sicherheit in LibreOffice“
59 BSI: „Leichter Einstieg“
60 BSI: „IT-Grundschutz, Informationssicherheit mit System“
61 Quelle: „13. Tätigkeitsbericht des Bayrischen Landesamts für Datenschutzaufsicht“
62 Quelle: Google / Android Hilfe: „Datenschutzeinstellungen für Werbung auf Android-Geräten verwalten.“
63 Quelle: DSK: „Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist“
64 Quelle: GetApp / Nubera eBusiness SL, Barcelona/ München: „Cyberangriffe auf deutsche Unternehmen & Führungskräfte“
65 Quelle: moz://a: „Kann mein Chef meine ChatGPT-Anfragen lesen?“
66 Quelle: LDI-NRW „Outlook-Update synchronisiert E-Mails in die Cloud“
67 Quelle: heise online: „Microsoft verteilt das neue Outlook ab Januar an Business-Kunden“
68 Quelle: DATEX Hilfe Center: „Microsoft Outlook new und DATEV-Programme“
69 Quelle: GetApp: „Cyberangriffe auf deutsche Unternehmen und Führungskräfte: Tools und Tipps ...“
70 Quelle: BMF: „Fragen und Antworten zur Einführung der obligatorischen (verpflichtenden) E-Rechnung zum 1. Januar 2025“
71 Quelle: lexware Office: „DSGVO – Vertrag zur Auftragsverarbeitung“

ENDNOTEN NR.

72 Quelle: sevdesk: „Allgemeine Informationen zur Datenschutz-Grundverordnung bei sevdesk“
73 Quelle: Buhl/WISO: „Muster Auftragsverarbeitungsvertrag“
74 Quelle: DATEV: „Vereinbarung zur Auftragsverarbeitung“
75 Quelle: RND: „„Daisy“ treibt Scam-Anrufer in den Wahnsinn.“