Übersicht 2022 | Zum Datenschutz aufgefallen

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 der Grundlagen für nachhaltigen Erfolg.

Mein Ziel ist es, den Datenschutz einfach, praktisch und hilfreich zu vermitteln und zu gestalten. Von Datenschutzberater, Datenschutzberatung, Datenschutz-management bis zertifizierter, externer Datenschutzbeauftragter für Selbst-ständige, Gewerbetreibende und KMU.

Es gilt die abstrakten, rechtlichen Anforderungen der DS-GVO und des BDSG in konkrete technische und organisatorische Maßnahmen umzusetzen, zumal höchstrichterliche Entscheidung noch folgen.

Information zum (Weblink)

Datenschutz - Service

oder Fragen per Mail an:

Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammenge stellt und beruhen auf öffent lich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.

Eine einfache, praktische Zusammenfassung und mehr, gibt es von mir als zertifizierter, extern Datenschutzbeauftragter über Datenschutzberatung bis Datenschutzmanagement.

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. 2.0b

Das SDM [der Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder (DSK)] überführt die rechtlichen Anforderungen der DS-GVO über 7 Gewährleistungsziele in die geforderten technischen und organisatorischen Maßnahmen zur Unterstützung der Transformation abstrakter – rechtlicher Anforderungen in konkrete Maßnahmen. Ziel ist eine gemeinsame Sprache der Juristen und Informatiker für die Verantwortlichen und Datenschutzpraktiker zu finden.

	Zusammenfassung SDM (10 Seiten)		Link DS-GVO auf dejure.org
	Link zum SDM der Aufsicht (72 Seiten)		Link BDSG auf dejure.org

Letzte Ergänzung: 11/2021: Baustein 51 (zu TOM)

Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“ (V.1.0 / 01.11.2021 / 23 Seiten)[1]. Kurze Zusammenfassung (1. Seite) und ein Richtlinienentwurf (2. Seiten), falls wünschenswert[2].

Sorry! Am 24.12.2022 teilt die DSK mit, dass eine neue Version 3.0 veröffentlicht wurde. Nach einem Überflug sind es Vereinfachungen und Verschlankungen. Dazu erst im Laufe des nächsten Jahres mehr 😐

Inhalte Monat@ 2022 *(Einfach Thema mit <Strg+F> suchen, oder direkt hier anklicken)*

(1) 🖹 ➔ **01@2022**

(2) Zum Datenschutz

(a) Patienten – Daten – Schutz – Gesetz (PDSG)

Das Ärzte, Labore und Kliniken bereits einen hohen (mehrheitlich internen) Digitalisierungsgrad aufweisen, haben leider die Cyberangriffe der letzten Jahre gezeigt. Auf der anderen Seite besteht ein erheblicher Mangel in der digitalen Kommunikation mit Dritten, z. B. mit den Patienten. Daraus folgt die Forderung nach: ***„Transformation, aber mit Sicherheit!“***, zumal Datenschutz-Grundverordnung (DS-GVO) und Bundesdatenschutzgesetz (BDSG) medizinische Daten unter besonderen Schutz gestellt wissen wollen. Festgehalten im fünften Buch der Sozialgesetzgebung Kapitel 10 und 11 (Abk. SGB V §284ff und §306ff)[3]. Einen kurzen Überblick der wesentlichen Inhalte gibt es hier – wie immer mit Angaben zu Quellen und Link - als PDF aus 3 Seiten: https://volkerschroer.de/DSGVO/2022.01.10.PDSG-kurzgefasst.pdf.

i) PDSG und Datenschutz

Bereits vor der Pandemie war der Ruf nach digitaler Transformation im Gesundheitswesen groß und die Diskussion um die Sicherheit der Daten aus allen Richtungen groß und führte zu Änderungen des ersten Entwurfs. Im Bundesgesetzblatt 2021 Teil 1 Nr. 28 vom 08.06.21 ist sogar eine Datenschutz – Folgenabschätzung als Anlage zu §307 mitveröffentlicht[4]. Mit Schreiben vom 16/8/21 hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI Prof. U. Kleber) einen Musterbescheid an die gesetzlichen Krankenkasse verschickt und eine Pressemitteilung am 19/8/21 veröffentlicht[5].

ii) Gesetzeskonflikte oder Umsetzungsmangel?

(Umsetzungsmangel!) Wenn ich die Veröffentlichungen des BfDI richtig deute, dann liegt es an:

1. Das (sich verzögernde) fehlen eines „feingranularen Berechtigungsmanagement“, mit der Versicherte / Patienten den Zugriff bzw. die Freigaben bis auf jeden einzelnen Datensatz selbst regeln können, da die gemantik GmbH (zuständige für die sichere Telematikinfrastruktur) noch kein System freigegeben hat. Was ja noch kommen kann!

2. Die „sichere digitale Identität“ ist spätestens ab dem 01.01.2023 (SGB V §291) verfügbar zu machen, d. h. es ist noch etwas Zeit, bis ein geeignetes System gefunden wird.

Korrekt ist, dass derzeit ohne Frontend (Kartenlesegerät, Smartphone) ein Zugriff nicht möglich ist. Da finde ich den Vorschlag eines Zugriffs über ein Kartenlesegerät in den Filialen der Krankenkassen eine geniale Alternative.

Die Aufbewahrungsfristen für die Leistungserbringer (Krankassen, Ärzte usw.) für die notwendigen Abrechnungsdaten sind ja geregelt und alle anderen Dokumente werden ja vom Versicherten / Patienten selbst verwaltet. Eine elektronische Patientenakte basiert auf Freiwilligkeit und muss bei der Krankenversicherungen beantragt werden.

Also weniger ein Gesetzeskonflikt zwischen PDSG und BDSG / DS-GVO, als ein noch zeitlich, lösbarer Umsetzungsmangel (hoffentlich?!).

iii) IT – Sicherheit zum Patienten - Datenschutz

Im Gesetz als Telematik – Infrastruktur bezeichnet. Die von der gematik GmbH (Umsetzungsgesellschaft des Bundes und der Leistungserbringer) konzipierten Anwendungen werden mit dem Bundesbeauftragen für den Datenschutz und die Informationsfreiheit (BfDI) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) abgestimmt, auf der Grundlage des SGB V Kapitel 11. Damit das in den Konzepten geplante Sicherheitsniveau auch in der Umsetzung gewährleistet werden kann, zertifiziert das BSI wichtige Komponenten, nachdem die einzelnen Komponenten von anerkannten Prüfstellen nach den Schutzprofilen und technischen Richtlinien des BSI[6] evaluiert wurden[7].

(b) Angst vor dem Kunden?

Datenschützer und Verbraucherverbände gehen gegen die Datenweitergabe von Mobilfunkanbietern vor, berichtet die Tagesschau[8]. Ohne Aufklärung der Verbrauchers / Nutzers, geschweige

denn einer Rechtsgrundlage, geben Mobilfunkanbieter (ohne die Telekom) Kundendaten (nicht Telefonate, sondern beispielsweise zum Vertragsabschluss, Vertragsdauer oder Vertragswechsel) an die Schufa weiter, zur Bewertung des Zahlungsverhaltens. „Warum werden wir nicht aufgeklärt? Da stimmt doch was nicht? Wo ist das Problem?“ Heimlichkeiten sind keine gute Strategie!

(3) Zur Datensicherheit

(a) IT-Sicherheit im Gesundheitswesen(?)

In der „Sektorstudie Gesundheit“ des BSI[9] vom 22.11.2021, gibt es unter Punkte 6 auf den Seiten 170ff, eine Liste von Empfehlung zur Verbesserung der Sicherheit der IT im Gesundheitswesen an Betreiber, Innenministerium, Gesundheitsministerium, Bundesregierung und Verbände. Als akuten, technischen Handlungsbedarf (Probleme) sieht das BSI die Absicherung von

unkontrollierten Fernwartungszugängen, potentielle Schwachstellen in IT-basierten, insbesondere vernetzten Medizinprodukten, der Netzwerkzugangskontrollen / Mobil Device Management, medizinische wie nicht – medizinische Netzwerke und die Verschärfung der Anforderungen an Zutritts- und Zugriffskontrollen.

(4) Zu angrenzenden Themen

(a) Aufsicht (AT): Google Analytics # DS-GVO [10]

Die österreichische Datenschutzbehörde hat einen (noch nicht rechtskräftigen) Bescheid zur Nutzung von Google Analytics durch Website – Betreiber erlassen. Durch die Nutzung des Tools auf der eigenen (verantwortlichen) Website entsteht ein einzigartiger, digitaler Fingerabdruck. Mangels Angemessenheitsbeschluss der EU und Maßnahmen für ein gleichwertiges Schutzniveau (schwer) ist ein Drittlandtransfer nicht erlaubt (Zitat: *„jedenfalls auf Grundlage des im Bescheid festgestellten Sachverhalts“*).

(b) Datenlecks in Schlagzeilen

Wie Tagesschau / Plusminus berichten[11], waren sensible Nutzerdaten von großen Plattformen OTTO, Kaufland, MediaMarkt, check24; Tyre24, idealo, Hood und Crowdfox jahrelang ungeschützt im Netz. Der Fehler wurde zwar 2021 behoben, die Daten (Mail- und Postadressen, Bestellinformationen, Telefonnummern, teilweise sogar Bankverbindungen) sind aber bereits im Darknet aufgetaucht. Betroffen sind ca. 700.000 Kunden. Die Plattformbetreiber verweisen zur datenschutzrechtlichen Haftung auf die Händler, sie seien ja nur Vermittler zu den Kunden ☹

(c) Datenpannen abseits der Schlagzeilen[12]

Es sind wohl nicht nur die „Großen“, denen Datenschutzverletzungen unterlaufen. Der LfDI – Schleswig – Holstein zieht das Fazit: „Wieder mehr Beschwerden, wieder mehr Datenpannen und vor allem mehr Angriffe auf den Datenschutz“. Die genannten Dauerbrenner:

- ✗ Home-Office: Weiterleiten von E-Mails an das private Mail – Konto
- ✗ Videoüberwachung: Fehlender u/o korrekter Hinweis, Löschroutine
- ✗ Corona Kontaktdaten: Von Dritten einsehbar, zusätzliche Informationen, Zweckentfremdung
- ✗ Unzureichende IT-Sicherheit: keine Verschlüsselung, Rücksicherungsmöglichkeit, Diebstahl
- ✗ Fehlversand/Verlust: Falscher Adressat und falscher Umgang bei Entdeckung
- ✗ Offene E-Mail-Verteiler und Umgang bei Entdeckung

(d) Feature?: Krypto-Miner von Avira & Norten

Doch bemerkenswert fand ich den Hinweis von WinFuture[13] unter Bezug auf mehrere andere Quellen, dass Norton und Avira über ihre Sicherheitssoftware auch Crypto - Miner installieren, die sich im Leerlauf ihres Rechners den Kapazitäten bedienen. Die Ankündigung (evtl. Zustimmung?) haben viele Nutzer anscheinend nicht bemerkt. Über die Höhe der Einnahmen, geschweige den eines Nutzeranteils ist bisher nicht bekannt.

(1) 🖂 ➔ **02@2022**

(2) Zum Datenschutz

(a) Mitarbeiter Information & Einwilligung(en)

Ein immer wieder gerne aufgegriffenes Thema ist die Verarbeitung von Mitarbeiterdaten einschließlich Fotos.

i) Datenschutzinformation

Unabhängig von der Rechtsgrundlage ist dem Mitarbeiter – immer – über den Datenschutz und die – konkrete – Datenverarbeitung eine Datenschutzinformation zur Verfügung zu stellen (Art.13, 14 DS-GVO)! Außer bei Groß- / Massenveranstaltungen können die grundsätzlichen Pflichtinformationen separat öffentlich, zugänglich gemacht werden (Aushang, Link, QR-Code).

ii) Rechtsgrundlagen

Rechtsgrundlagen sind notwendige Daten für das Beschäftigungsverhältnis (§26 BDSG); ein berechtigtes Interesse[14] (Art.6 DS-GVO), wenn 1.) vorliegt?, 2.) erforderlich und kein milderes Mittel verfügbar? 3.) Abwägung mit den Interessen des Betroffenen (z. B. Fotos im Internet scheiden wegen Unkontrollierbarkeit der weiteren Verwendung aus); separater Vertrag mit Gegenleistung (eher selten, z. B. Modell – Agentur) und

iii) Einwilligung

Die Einwilligung[15] (nach Art.7 DS-GVO) muss für jeden konkreten Fall, in informativer und unmissverständlicher Weise für jeden Fall „freiwillig“ und ohne Nachteil bei einer Ablehnung erteilt werden. Die Schriftform ist zur Nachweispflicht sehr zu empfehlen!

Eine Vorlage für die Datenschutzinformation an die Mitarbeiter und für eine Einwilligung von Mitarbeitern am Beispiel Fotoaufnahmen finden Sie als PDF Stand: Februar 2022 hier:
https://www.volkerschroer.de/DSGVO/2022.02.25.Vorlage.Datenschutz.Information.Mitarbeiter.Einwilligung.pdf

(b) Koordinierte Prüfung von Cloud – Diensten durch EU – Aufsichtsbehörden

Der Europäische Datenschutzausschuss (EDSA) bzw. die EU – Aufsichtsbehörden haben in einer koordinierten Aktion die Nutzung Cloud – basierter Dienste durch den öffentlichen Sektor gestartet. So die Pressemitteilung des BfDI[16] und des EDSA[5]. Dies betrifft zunächst wohl nur den öffentlichen Sektor, die aggregierten Ergebnisse dürften aber mit Sicherheit Auswirkungen auf den nicht – öffentlichen Sektor haben. *PS: 06/2021 Aufsicht setzte Behörden eine Frist für Facebook Nutzung.*

(c) Websites & Medienstaatsvertrag[17]

Mit dem Medienstaatsvertrag (11/2020) wurde der Rundfunkstaatsvertrag zwischen den Bundesländern ersetzt. (Website Angabe ALT: „§55 RStV“ – NEU: „§18 MStV“) um die gesamte Medienwelt einschließlich Medien - Intermediäre abzudecken (z. B. Plattformbetreiber wie Facebook, Google usw.), sowie die aggregierten, selektierten und / oder präsentierten journalistisch - redaktionellen Angebote Dritter. Was ist für Betreiber von Websites neben dem Gesetzesbezug neu zu beachten:

- ✔ Angabe von Name, Vorname und Adresse des/der Verantwortlichen
- ✔ Bei juristischen Personen die Angaben des Vertretungsberechtigten (§18 Abs.1 Nr.2)
- ✔ Verantwortliche(r) mit ständigem Wohnsitz in Deutschland (unbeschränkt strafrechtl. verfolgbar)
- ✔ Einhaltung journalistischer Sorgfaltspflichten (Wahrheitsgehalt, repräsentative Umfragen usw.)
- ✔ Bots, die Inhalte, Beiträge oder Chats automatisiert erstellen, sind kennzeichnungspflichtig!

(d) „Nur“ €100 Schmerzgeld, aber Urteil mit Folgen?[18]

Im Tenor wird dem Websitebetreiber zur Bereitstellung von Schriftarten über eine Schnittstelle (hier API zu Google Fonts in die USA, als unsicherer Drittstaat nach DS-GVO) die Übermittlung der IP-Adresse (als personenbezogenes Identifikationsmerkmal) an diesen Anbieter untersagt. Das Schmerzensgeld beträgt 100€, bei Zuwiderhandlung drohen aber bis zu 250.000€, ersatzweise bis zu 6 Monaten Ordnungshaft ☹.

- ✔ Unstrittig ist der Personenbezug einer IP-Adresse, ob statisch oder dynamisch[19]

i) ?Berechtigtes Interesse der Verantwortlichen (Art.6 Abs.1 f DSGVO)?

✔ Abwägung der rechtlichen, tatsächlichen, wirtschaftlichen und ideellen Interessen: Dies kann angenommen werden, da eine ansprechende Darstellung durch attraktive Schriftarten im wirtschaftlichen Interesse liegt.✔

✗ Erforderlichkeit mangels eines milderen, gleichwertigen, effektiven Mittels: Gleicher Effekt hätte durch herunterladen der Schriftarten auf den eigenen Server erzielt werden können.✖

● Abwägung der Interessen des Verantwortlich gegen mögliche überwiegende Interessen, Grundrechte oder Grundfreiheiten des Betroffenen: Prüfung wegen mildere Alternative hier nicht mehr erforderlich.

ii) ?Einwilligung (Art.6 Abs.1 a; Art.12; Art.49 Abs.1 a DSGVO)?

➔ Die Einwilligung erfordert eine transparente Information, Kommunikation und vor allem die Modalitäten für die Ausübung der Rechte der betroffenen Person, was vor dem Aufruf der Seite schwerlich darzustellen ist. Die Einwilligung in die Übermittlung (der IP-Adresse) in ein unsicheres Drittland ist als Ausnahme und nicht systematische und wiederholende nach der DS – GVO vorgesehen.✖

➔ Im übrigen schreibt auch das Telemedien – Telekommunikation – Datenschutz – Gesetz (in §25 Abs.1TTDSG) vor *„Die Speicherung von Informationen in … oder der Zugriff auf Informationen ... in der Endeinrichtung ... sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat.“* Unmöglichkeit der Einwilligung, da IP-Adresse, Gerätedaten bereits mit dem ersten Aufruf an Google gehen. ✖

(3) Zur Datensicherheit

(a) Herstellerhaftung für Software – Mängel

Die Bundesregierung will dafür sorgen, dass Hersteller künftig für Schäden haften, die fahrlässig durch Software-Schwachstellen in ihren Produkten entstanden sind. Das kündigte Bundesinnenministerin Nancy Faeser (SPD) am Dienstag beim 18. Deutschen IT-Sicherheitskongress an. Der Chaos – Computer – Club hatte bereits für das Regierungsprogramm formuliert: *„Die Bundesregierung will dafür sorgen, dass Hersteller künftig für Schäden haften, die fahrlässig durch Software-Schwachstellen in ihren Produkten entstanden sind.“*[20] Die IoT Security Foundaton hatte in einer Untersuchung festgestellt, dass 80% der IoT – Geräte - Hersteller gar nicht oder nur unzureichend auf Sicherheitsmängel reagieren.[21] Es wird Zeit !!!.

(4) Zu angrenzenden Themen

(a) Ihre biometrischen Daten im Angebot?

Aus dem WDR – Clip[22] mit obigen Titel geht hervor, dass viele App – Anbieter hochgeladene Fotos zu Geld machen, ohne deutlichen Hinweis zu einer Einwilligung. Meta/Facebook hat gerade 1 Milliarde solcher Daten gelöscht. Auf der Seite mobilsicher.de[23] wurden Beauty – Apps darauf getestet, viele davon geben die Daten an viele Interessenten weiter (Score 4 = hohes Risiko). Ein Datenschutz – Fachbeitrag zu biometrischen Daten in diesem Zusammenhang kommt von Dr.Datenschutz: *„Beauty Apps und Datenschutz: Wer schön sein will, muss leiden“*[24]

Dazu passt ein Artikel in der Süddeutschen Zeitung: „Der Albtraum für die Privatsphäre: Das Programm "Clearview AI“[25], deren Datensauger liest alle öffentlich, zugänglichen Netze aus und liefert bei Übereinstimmung auch weitere, personenbezogene Daten. Laut einer Investoren-konferenz liegt der Bestand bei 10 Mrd. Personendaten und soll bis Ende des Jahres auf 100 Mrd. ansteigen (so der Spiegel[11]). Was bisher „nur“ von Behörden genutzt wird, soll laut Unternehmens - Präsentation auch Privatunternehmen angeboten werden, was kurz danach und zunächst wohl auf Grund des Aufschreis dementiert wurde. Zudem stellt sich die Frage, wer die Sicherheit der Systeme und die Einhaltung der Regularien überprüft. Es ist zu hoffen, dass kurzfristig eine Regulierung erfolgt, damit nicht jeder, jeden überprüfen kann, wenn ein Kamera in der Nähe ist ☹.

(1) 🖻 ➔ **03@2022**

(2) Zum Datenschutz

(a) (Teilakt-) Fotos aus der Vergangenheit (?→!)

Ein Fall aus dem Tätigkeitsbericht 2022, Punkt 5.4. der Datenschutzaufsicht Schleswig-Holstein[26] .

i) Der Fall:

Der Betroffene hatte vor 10 Jahren an einem Fotoshooting mit „normalen“ Bildern und einem Teilaktbild teilgenommen, dafür zusätzliche Fotodaten auf CD und ein Poster im Wert von 190€ erhalten und wurde jetzt von Kollegen auf dieses Teilaktbild hingewiesen.

ii) Die Entscheidung

Aufgrund der schriftlichen, vertraglichen Regelung (man spricht hier von Modell – Vertrag), die damals nach gültigem BDSG und heutigem Art.6 Abs.1b DS-GVO rechtmäßig war und ist, wurde von etwaigen Maßnahmen durch die Aufsichtsbehörde abgesehen.

iii) Fazit:

Wer für die Einwilligung in ein umfassendes und vielleicht sogar unbefristetes Bildnutzungsrecht eine Gegenleistung erhält, sollte die Zustimmung dazu sehr gut abwägen. Der Fotograf sollte die Einwilligung *„hinreichend bestimmt und in einer verständlichen, klaren und einfachen Sprache formulieren.“*

(b) Werbung VOR Einwilligung (Privat/Gewerbe), geht das?

Die Datenschutznord-Gruppe greift in ihren Datenschutznotizen die Frage auf: *“Die große Werbekampagne per Briefpost – zulässig?“* [27].

i) Anlass:

Ein großer Konzern macht in Hamburg Werbung mit einer Postwurfsendung („Postwurfspezial“)[28] als teiladressierte Werbung (z.B. An Haushalte der Stadt, Region, Bezirk usw.), d. h. ohne konkrete bzw. aus Empfängerkreis ermittelbare Personenangaben, keine Informationen zum Datenschutz, mit Hinweis zu einer App und einem individuellen Rabattcode für die erste Bestellung.

ii) Datenschutz (DS-GVO)

JA, bei Werbung per Post ohne Angaben zu personenbezogenen Daten bzw. deren Verwendung, findet keine Verarbeitung von personenbezogenen Daten statt und die Regelungen der DS-GVO sind für die Empfänger nicht anwendbar. BEACHTUNG: Natürlich müssen Widersprüche, z. B. Briefkastenaufkleber: „Bitte keine Werbung“ u. ä. beachtet werden.

ABER WENN ein Personenbezug (vorher wie nachher) zum Beispiel über einen tatsächlichen, individuellen Rabattcode u. ä. hergestellt werden kann, findet eine Verarbeitung nach DS-GVO statt und die Regelungen sind anwendbar (Informationspflichten u.s.w.). Bei einer Erstwerbung könnte anstelle einer Einwilligung vorab auf die „Wahrung der berechtigten Interesse des Verantwortlichen“, sofern nicht die Interessen der Betroffenen überwiegen, nach Art.6 Abs.1f und Erwägungsgrund (47) abgestellt werden. In der Orientierungshilfe der Datenschutzkonferenz zur Direktwerbung lautet es dazu u. a.: „*Die DS-GVO verlangt eine Abwägung im konkreten Einzelfall … muss ferner insgesamt im Hinblick auf die Wahrung der berechtigten Interessen erforderlich sein. … Damit ist auch auf die subjektive Erwartungshaltung der betroffenen Person im Einzelfall abzustellen.*“ Es kommt also auf den zu prüfenden Einzelfall und kommende Gerichtsentscheidungen an.

iii) Wettbewerbsrecht (UWG)

Der Fokus liegt hier auf §7 UWG unzumutbare Belästigungen, der im Schwerpunkt auf elektronische Kommunikation (Telefon, E-Mail u.ä) abstellt. „*Dies gilt insbesondere für Werbung, obwohl erkennbar ist, dass der angesprochene Marktteilnehmer diese Werbung nicht wünscht.*“ Verkürzt gesagt kann Werbung nur mit Einwilligung und in verständlicher und transparenter Form erfolgen. Ausnahmen bestehen im Rahmen der Datenerhebung in Verkaufsprozessen auch für ähnliche Waren mit Informationspflicht und Widerspruchsrecht.

B2B Nach Ausführungen der Wettbewerbszentrale[29] genügt nach §7 Abs.2 Nr.2 UWG für die Telefonwerbung (und auch nur für diese) mit Unternehmen die *„mutmaßliche Einwilligung“*. Diese ist gegeben, wenn aufgrund konkreter tatsächlicher Umstände ein sachliches Interesse des Anzurufenden an der Telefonwerbung vermutet werden kann. Der BGH führt dazu bereits mehrfach aus[30]: *„Bei der Beurteilung der Frage, ob der Anrufer von einer mutmaßlichen Einwilligung des anzurufenden Gewerbetreibenden ausgehen konnte, ist auf die Umstände vor dem Anruf sowie auf die Art und den Inhalt der Werbung abzustellen. Maßgeblich ist, ob der Werbende bei verständiger Würdigung der Umstände annehmen durfte, der Anzurufende erwarte einen solchen Anruf oder werde ihm jedenfalls positiv gegenüberstehen.“*

iv) Werbebrief und Postwurfsendung

B2B + anonymisiert sind erstmalige Werbebriefe (Flyer) demnach zulässig, solange der Empfänger nicht widerspricht, z. B. durch einen Briefkastenaufkleber oder direktem Widerspruch beim Versender.

B2C sind erstmalige Werbebriefe (Flyer) demnach zulässig, solange der Empfänger nicht widerspricht, z. B. durch einen Briefkastenaufkleber oder direktem Widerspruch beim Versender. **WENN** die Adresse aus einer öffentlichen Quelle stammt und der Empfänger mit den Informationspflichten[31] über Herkunft, Zweck und Widerspruchsmöglichkeit informiert wird.

v) PS: Visitenkarten

www.openclipart.org

Wo ich gerade bei der Orientierungshilfe der Datenschutzkonferenz zur Direktwerbung[32] bin, ist da auch unter „3.2“ ein Eintrag zu „Einwilligung mit Übergabe von Visitenkarten“. Zitat spricht für sich: „*Visitenkarten, die von den betroffenen Personen auf Messen oder sonstigen Veranstaltungen ausdrücklich zur Informationszusendung oder weiteren geschäftlichen Kontaktaufnahme hinterlassen werden, können grundsätzlich eine wirksame Einwilligung im Sinne von Art. 4 Nr. 11 DS-GVO darstellen, wenn infolge der Umstände des Einzelfalls für den Verantwortlichen eine Nachweisbarkeit der Einwilligung und insbesondere auch ihres Inhalts gegeben ist.*“ Man kann natürlich im Nachgang eine Bestätigung per E-Mail schreiben um 100% sicher zu sein. (?) Zumindest ist der „Umstand“ kurz, für mögliche Nachfragen, festzuhalten. Bei erster Nachricht den Widerruf nicht vergessen.

vi) PS: E-Mail-Signatur mit Werbung

www.openclipart.org

Werbliche Zusätze (1 Satz reicht) zur E-Mail-Signatur ohne Werbeeinwilligung können „eine Verletzung des allgemeinen Persönlichkeitsrechts darstellen“ (BGH 2015:VIZR 134/15 & [33].)

(3) Zur Datensicherheit

(a) „Ice-Phishing“ (Blockchain, Web3.0) [34]


www.freepic.com

Begriffliche Ableitung vom Eisfischen. Zu den bisherigen Phishing - Methoden **Speer – Phishing** (Vortäuschen eines vertrauenswürdigen Kommunikationspartners per Web, Mail, Kurznachrichten), **Social Engineering** (Psychologische Manipulation zur Preisgabe vertraulicher Informationen oder Geldzugang) und **Executive Whaling** (gezielte, aufwendige, personalisierte Manipulation von Führungskräften, zur Preisgabe vertraulicher Informationen oder Geldzugang) gesellt sich nach Berichten von Microsoft das **Ice – Phising**, insbesondere als Bedrohung von Blockchain, Web 3.0 (Innovation des Internets, das auf der Blockchain basiert und Konzepte wie Dezentralisierung und Token-basierte Wirtschaft beinhaltet) und DeFi (Decentralized Finance mit Smart Contracts). Anders als bisher ignoriert die Angriffsmethode private Schlüssel, sondern verleitet den Anwender die Genehmigung für die Übertragung eines Token zu erteilen. Empfänger ist dann der Angreifer.

Fazit: Die bekannte Regel gilt auch hier, wenn möglich, immer direkt eine Anwendung aufrufen und möglichst nie aus einer Nachricht oder einem Link – Angebot!

(4) Zu angrenzenden Themen

(a) BSI warnt vor der Produkten der Security Suite von Kasparsky. [35]

Gefährdet seien Nutzer der Software und Unternehmen. Ein russischer IT-Hersteller könne "selbst offensive Operationen durchführen, gegen seinen Willen gezwungen werden, Zielsysteme anzugreifen, oder selbst als Opfer einer Cyber-Operation ohne seine Kenntnis ausspioniert oder als Werkzeug für Angriffe gegen seine eigenen Kunden missbraucht werden".

(1) 🗃 ➔ **04@2022**

(2) Zum Datenschutz

(a) Immer wieder Facebook😐

i) Vorbemerkung

Immer wieder Facebook – Fanpage im Fadenkreuz der Aufsicht des Datenschutzes und kein Ende. Das betreiben einer Facebook – Fanpage bietet Vorteile, wie eine weite Verbreitung, die schnelle Resonanz mit direktem Feedback und die Suchmaschinenaufmerksamkeit. Die Nachteile sind Zeitaufwand und Langfriststrategie, um mit regelmäßigen Beiträgen die Aufmerksamkeit der „Follower“ auf hohem Niveau zu halten, damit der Seite nicht die Verwaisung droht. Hinzu kommt nach Aussagen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sowie der Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder (DSK), dass ein datenschutzkonformes Betreiben einer Fanpage derzeit nicht (zu 100%) möglich ist. In der Fußnote sind einige Artikel vom BfDI zum Nachlesen aus Juni 2021 verlinkt[36]. An dem Status hat sich auch bis heute nichts geändert. 😐

ii) Datenschutz & Facebook

A. Die drei Fragen des Datenschutzes:

1) Transparenz: Ist der Nutzer leicht und vollumfänglich über Art, Zweck und Dauer informiert?
2) Nutzerrecht: Können die Rechte nach DS-GVO (z. B. Löschen, Widerspruch) erfüllt werden?
3) Vertraulichkeit: Ist diese je nach Sensibilität, Integrität und Verfügbarkeit gewährleistet?

Die Fragen sind sicherlich nicht alle mit einem eindeutigen „JA“ zu beantworten!

B. Meta/Facebook und das Datensammeln:

1) Viele Daten erhält Facebook aus der Anmeldung (Kontaktdaten & freiwillige Angaben)!
2) Aus den Zugriffsfreigaben auf jedem Telefon (z. B. Adressbuch, wer-mit-wem)!
3) Weitere Daten aus den „Post“ der Nutzer (Text, Bilder, Telefon, Standort u. v. m.)!
4) Aus den „Likes“, dem Surfverhalten der Nutzer und Dritten (z. B. über IP–Adresse & Cookie)!

und noch einiges mehr an Daten[37] und wissen nicht mal, was sie genau damit machen[38] (siehe auch Fußnote). Deshalb hatte schon ein belgisches Gericht die Praxis, insbesondere bei „unbeteiligten“ Dritten mangels ausreichender Information untersagt und mit 250.000€ / Tag Strafe gedroht.[39]

5) Nach dem bekannten „Schremms II“ Urteil kommen Einschränkungen aus US-Rechte hinzu!
6) Immer wieder Datenpannen (Cambridge Analytics 2018; ungeschützte Nutzerdaten 2019)
7) Laufende Aufsichtsverfahren, mittlerweile nicht mehr nur in Irland.

C. Gemeinsame Verantwortung

Bereits in 2018 hat der Europäische Gerichtshof (EuGH Aktz: C-210/16) eine gemeinsame Verantwortlichkeit von Facebook und dem Fanpage – Betreiber festgestellt. Nach Art.26 DS-GVO ist eine Vereinbarung / Vertrag zu schließen[40] (Siehe auch Erläuterung und Muster unter[41])

iii) Resümee:

Ein 100% datenschutzkonformes Betreiben einer Facebook – Fanpage ist auch nach Aktualisierung des Page Controller Addendums[42] (Nachtrag Seitenverantwortlicher) durch Facebook nicht darstellbar. Unter Einhaltung der aufsichtsrechtlichen Vorgaben und Hinweisen sollte eine Risikoabwägung der Vorteile mit den möglichen Gefahren (Abmahnung bis Stilllegungsanordnung) vorgenommen werden, sofern nicht auf einen Betrieb verzichtet werden kann.

iv) Wenn es den Facebook sein muss (!)

Anleitung zum Impressum, Datenschutz und einen Textentwurf (ab Seite 2) finden Sie hier: https://volkerschroer.de/DSGVO/2022.03.21.Meta-Facebook-Fanpage-Datenschutz.pdf

Bildquelle: https://joinmastodon.org/

v) Alternativen eine Chance geben (!!!)

„Mastodon“[43], dass Elefanten – Netzwerk, „Toots“ statt „Tweets“. Schon mal gehört? Dezentrales statt zentrales Netzwerk, werbefrei und damit kein Datensammler und Profilersteller. Die Anmeldung erfolgt über einen der Knotenpunkte (Liste der Instances in der Fußnote). Im Playstore gibt es eine passende App für das Smartphone (Link zum Original). Die Bundesbehörden setzen bereits darauf, der gesamte öffentliche Bereich wird folgen und die Übernahme von Twitter durch Elon Mask hat für weiteren Zulauf gesorgt. Und Schwarmverhalten (z. B. kollektive Wachsamkeit) führt zu kollektiver Intelligenz (Schwarmverhalten)[44]. Die „Anderen“ werden sicher folgen!

(b) CISPE & EU Cloud CoC?

Der Datenschutzkodex für Anbieter von Cloud – Infrastruktur - Services in Europa (CISPE) und der EU Cloud Code of Conduct (EU Cloud CoC) sind paneuropäische Datenschutz-Verhaltenskodexe für Anbieter von Cloud – Infrastruktur - Services und können als Faktor herangezogen werden, um hinreichende Garantien bei der Einhaltung der Anforderungen an den Auftragsverarbeiter oder die Erfüllung der Anforderungen an die Sicherheit der Verarbeitung gemäß DS - GVO nachzuweisen.[45]

(3) Zur Datensicherheit

(a) Verfassungsschutz warnt vor russischen Cyberangriffen

Wie CSO-Online berichtet, gibt es „Neue Warnung des Verfassungsschutzes vor russischen Cyberattacken“[46]. Es wird um erhöhte Vorsicht gebeten gegen Phising - Mails der Ghostwriter – Gruppe des russischen Geheimdienstes. Außerdem sollten Gesprächen über die beruflichen Tätigkeiten mit äußerster Zurückhaltung geführt werden.

(b) Auflegen: Wenn Microsoft anruft (!)

Wie nicht nur der Spiegel berichtet[47], erfolgen wieder verstärkte Anrufe von *angeblichen Microsoft – Mitarbeiter* nach der alten Masche, um einen wichtigen Fehler im Betriebssystem beheben zu wollen braucht man aus *„Sicherheitsgründen“* die Mitarbeit vor Ort. Dazu muss *„natürlich“* eine Fernwartungssoftware freigeschaltet werden, womit die Betrüger den internen Blick auf Daten und Systeme erhalten. Schutzmaßnahme: „AUFLEGEN“, so etwas macht Microsoft (& andere) nicht!

PS: Sicherheit ist ein Dauerbrenner, laut Bericht des BSI zur IT-Sicherheitslage[48] in 2021 stiegen die Schadprogramm – VARIANTEN um 22% auf 144 Mio. (= 394.000 Varianten pro Tag im Ø).

(4) Zu angrenzenden Themen

(a) Frühjahrsputz

Der Frühling ist da und ein Frühjahrsputz kann auch in der IT, dem PC und Mobilgeräten nicht schaden. Löschen Sie was gelöscht werden muss und kann, wie Daten, Dateien, Ordner und Anwendungen, die nicht benötigt werden, oder lange nicht mehr gebraucht wurden! Das spart Platz und schließt gleichzeitig potentielle Sicherheitslücken. Dabei können verbleibende Anwendungen gleich auf Aktualität und automatischer Update – Funktion geprüft werden – wenn Sie schon dabei sind.

(b) Sieh an, die Schufa![49]

Die Schufa erläuter ihr Scoring, zumindest in großen Teilen. Die eigentliche Berechnungsmethode bleibt aber Betriebsgeheimnis und ist „nur“ den Datenschutzbehörden offengelegt. Aber, immerhin erfahren wir, dass gerichtliche Entscheidungen (Vollstreckungstitel, Mahnbescheide, eidesstattliche Erklärungen, Insolvenzverfahren, Restschuldbefreiung) so ein Saldo nach Gesamtfälligstellung den Score negativ beeinflussen. Positiv wirken Kredithistorie, Vorleistung wie Girokonto, Kreditkarte, Bürgschaften, Ratenkredite, Leasing u. ä., auch Anfragen dazu. Häufige, zeitgleiche Anfragen bei unterschiedlichen Anbietern wirken negativ, sofern es keine Konditionsanfragen sind.

(c) Beweislast bei E – Mail versandt.

Das Landesarbeitsgericht in Köln schreibt unter AZ: 4 Sa 315/21[50]: *„Den Absender einer E-Mail trifft gemäß § 130 BGB die volle Darlegungs- und Beweislast dafür, dass die E-Mail dem Empfänger zugegangen ist. Ihm kommt nicht dadurch die Beweiserleichterung des Anscheinsbeweises zugute, dass er nach dem Versenden keine Meldung über die Unzustellbarkeit der E-Mail erhält.“*

(1) 🗀 ➔ **05@2022**

(2) Zum Datenschutz

(a) Die dunkle Seite

… im Datenschutz als „DARK PATTERNS“ bezeichnet. Das bewusste (, aber nach der DS-GVO verbotene) einsetzen von Antimustern. Manipulative Designs sollen Nutzer* einer Website oder App dazu verleiten, unbeabsichtigte, unfreiwillige und möglicherweise schädliche Entscheidungen über die Verarbeitung ihrer Daten zu treffen (Richtlinie 3/2022 european data protection board)[51].

i) Dunkle Muster:

- *Überlastung (Overloading)* durch kontinuierliche Eingabeaufforderungen, Datenschutz-labyrinth oder zu viele Optionen.
- *Überspringen (Skipping)* durch Ablenkung mit täuschender Gemütlichkeit bzw. Ablenkung.
- *Rühren (Stirring)* mittels emotionaler Steuerung und in Sichtweite versteckt.
- *Behinderung (Hindering)* der eigentlich gewollten Nutzung durch Sackgassen, nervige Verzögerungen oder irreführende Informationen.
- *Unbeständig (Fickle)* durch unklare Benutzeroberfläche und Design zu Datenschutz – Kontrollinstrumenten durch mangelnde Einteilung oder unverständliche Zusammenhänge.
- *Im Dunkeln lassen (Left in the dark)*, durch verschleiern, verbergen, verstecken und verklausulieren der Datenverarbeitung und Rechte auf der Website.

Alle diese Muster (und weitere) widersprechen den Verarbeitungsgrundsätzen nach Art.5 DS-GVO, der Rechtmäßigkeit zu Transparenz und nach Treu und Glauben.

ii) Vermeidung

Verantwortliche sollten diese Muster vermeiden durch datenschutzfreundliche Voreinstellungen (Data Protection by Default) und datenschutzfreundlichen Technikgestaltung (Data Protection by design). Zur Systematisierung für Datenschutzpraktiker bietet das Standard – Datenschutz – Model übersichtlich die 7 Gewährleistungsziele an:

- Transparenz (Was, wofür, einfach und verständlich)
- Intervenierbarkeit (Eingriffsmöglichkeiten und Rechte, einfach und verständlich)
- Vertraulichkeit | Datenminimierung | Nichtverkettung | Integrität | Verfügbarkeit

Weiterführende Erläuterungen zu den Gewährleistungszielen sind auf der ersten Seite verlinkt. Die Richtlinie des edpb gibt auch passende, negative Beispiel wie:

„Hey, ein einsamer Wolf, bist du? Aber das Teilen und Verbinden mit anderen trägt dazu bei, die Welt zu einem besseren Ort zu machen! Teile deine Geolokalisierung! Lasse Dich von den Orten und Menschen um Dich herum inspirieren!“
„Du musst nicht erst zum Friseur gehen. Wähle einfach ein Foto aus, auf dem steht: ‚Das bin ich‘.“

Grundsätzlich gilt, wenn die Datenschutzinformation nicht, zu einfach oder unverständlich sind, sollten jeder ganz genau hinschauen und im Zweifel lieber abbrechen.

(b) Zensus 2022, Volkszählung

i) Zur Sicherheit

Wie tagesschau.de am 14.5.2022[52] berichtete, ist mit dem Urteil des BVerfG vom 15.12.1983[53] der Datenschutz entstanden. Damals wurde Teile der Volkszählung als verfassungswidrig angesehen. Der folgende Auszug aus dem damaligen Urteil erscheint mir sehr zukunftsweisend:

„Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. (…) Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. (…) Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

Die EU hat mit der Verordnung Nr.763/2008 Standards über Volks- und Wohnungszählungen erlassen. Darin werden in Artikel 4 zu Datenquellen herkömmliche und registergestützte Zählungen und Stichprobenerhebungen genannt und ergänzend in Abs.2 *„Die Mitgliedsstaaten ergreifen alle Maßnahmen, um die Anforderungen des Datenschutzes zu erfüllen.“*

Nach einer Pressemitteilung[54] des BfDI als Aufsichtsbehörde hat eine unmittelbare Prüfung keine Gefahr für die Sicherheit ergeben. Es hatte Irritationen bezüglich des Einsatzes eines US – Cloud - Anbieters in einem Teilbereich gegeben. Die Gesamtprüfung dauert allerdings noch an.

ii) Beantwortungspflicht?

Ja, die ist im Gesetz zur Durchführung des Zensus im Jahr 2022 in §§23ff[55] festgehalten, mit einer Geldbuße bei Verweigerung. Befragt werden neben den Haushalten auch die Vermieter*.

iii) Verfassungskonform?

Ja, in einem Urteil des BVerfG aus 2018 zum Zensus 2011 bestätigt[56]. Weiter Informationen und Videos auf zdf.de[57]

(3) Zur (IT-) Datensicherheit

(a) BSI – Lagebericht Deutschland

Der Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für 2021 ist überschrieben mit: *„Die IT – Sicherheitslage bleibt angespannt bis kritisch“*[58].Neue Varianten an Schadprogrammen stiegen gegenüber 2020 um 22% auf 144 Mio. Gründe für die Alarmstufe: ROT in Teilbereichen sind 1.) eine deutliche Professionalisierung der Cyberkriminalität, 2.) die zunehmende, digitale Vernetzung und 3.) eine weite Verbreitung gravierender Schwachstellen in IT – Produkten. Das volle Potential der Digitalisierung können wir nur nutzen, wenn wir die IT – Sicherheit dabei nicht vernachlässigen (Ausfallvermeidung, Vertrauen).

(4) Zu angrenzenden Themen

(a) BfDI – 30. Tätigkeitsbericht vorgestellt

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat seinen 30. Tätigkeitsbericht vorgelegt[59]. Themen die mir spontan ins Auge gefallen sind: Arbeitskreis mit Microsoft, also noch keine abschließende Klärung eines datenschutzkonformen Betriebs; ☑Der Datentransfer mit Großbritannien bleibt unverändert, da im Datenschutz die EU – Mitgliedschaft durch einen Angemessenheitsbeschluss bis Juni 2025 ersetzt wurde. Der BfDI sieht keinen Grund, die Veröffentlichung der E-Mail-Korrespondenz von Bundesminister Scheuer zur PKW – Maut einem Petent zu verweigern.

(b) Digitalführerschein (privat/beruflich)[60]

Eine im Bundestag beschlossene Initiative, gefördert vom Bundesinnenministerium und DsiN (Deutschland sicher im Netz), ist die Zertifizierung eines digitalen Führerscheins (mit Lernprogramm und Zwischenprüfung ☺).Ich habe es bisher nur „angetestet“, scheint sehr empfehlenswert.

(c) Big Brother Award 2022 geht an:

Die irische Datenschutzbehörde für ihr Lebenswerk der nachhaltigen Arbeitsverweigerung[61] und an die Klarna Bank AB zum Verbraucherschutz wegen intransparenter Bündelung von Daten aus Shop - Service, Zahlungsdienstleister, Preisvergleichsportal, persönlicher Finanzmanager, Bonitätskontrolleur und Bank[62].

(1) ➔ **06@2022**

(2) Zum Datenschutz

(a) Das Auskunftsrecht

i) EU – Grundrechtscharta

Schon hier ist in Art 8[63] festgehalten: *„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung“*

ii) DS-GVO (BDSG)

Und hier in Art. 15: *„(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, … so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:“*

iii) Grenzen DS-GVO (BDSG)

Betriebs- und Geschäftsgeheimnisse, geistiges Eigentum und Urheberrechte unterliegen nicht dem Auskunftsrecht, sofern der Verantwortliche die Kollision mit den Rechten und Freiheiten der Rechteinhaber nachweisen kann, gemäß Erwägungsgrund 63, Art. 15 (4) DS-GVO und §29 BDSG. (Beispiel: Risikoaufschlag einer Versicherung[64], Schufa-Scroing[65])
Gemäß §34 Abs.1 besteht das **Auskunftsrecht nicht, wenn** *„die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde **sowie** eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist“* **und eine Verarbeitung nur** aufgrund gesetzlicher, satzungsmäßiger Vorschriften, oder ausschließlich zum Zweck der Datensicherung noch Daten verarbeitet werden. → Was immer zu begründen ist!

iv) Richtlinien edpb, EU – Datenschutzausschuss [66]

Und jetzt hat der europäische Datenschutzausschuss noch eine 60 – seitige Richtlinie dazu ausgegeben mit dem Ziel, Einzelpersonen ausreichende, transparente und leicht zugängliche Informationen über die Verarbeitung ihrer personenbezogenen Daten bereitzustellen, damit sie die Rechtmäßigkeit der Verarbeitung und die Richtigkeit der verarbeiteten Daten kennen und überprüfen können. **Das Wesentliche:**

- Es Bedarf keiner Begründung für das Auskunftsersuchen.
- Pflicht zur Prüfung des korrekten Anfragenden, ggf. durch zusätzliche Anforderungen.
- Beantwortung spätestens innerhalb eines Monats, eine negative Beauskunftung ist zwingend. Ausnahme lediglich bei Eingang an völlig zufälligen oder offensichtlich falschen Adressen.
- Auskunft (in verständlicher und transparenter Form) über Zweck, Verarbeitung, Kategorien von Daten und Empfängern, Dauer, Betroffenenrechte und Besonderheiten bei Drittlandübermittlung zu gleichen Rechten.
- Der Umfang umfasste alle personenbezogene Daten (Kontaktdaten, IP-Adresse usw.) und die sich auf die Person beziehenden Daten (Befunde, Entscheidungen usw.), einschließlich der Daten von und mit Dritten (sofern deren Betroffenenrechte nicht überwiegen, was zu begründen ist). Dies schließt auch alle nicht digitalisierten und pseudonymisierte Daten mit ein, nur **anonymisierte Daten sind ausgenommen**.
- Information und Zugang in präziser, transparenter, verständlicher und leicht zugänglicher Form, sowie in einer klaren und einfachen Sprache, unter Berücksichtigung des Umfangs und der Fähigkeiten der anfragenden Person (z. B. Kinder, Personen mit besonderen Bedürfnissen).
- (!)Information über die Verarbeitung der Daten zur Auskunftsanfrage und Aufklärung über die Betroffenenrechte ist ein wichtiger Bestandteil und nicht zu vergessen.

v) Grenzfälle

- Kopie von ***Ausweisdokumenten*** zur Identifizierung stellen ein großes Sicherheitsrisiko für den Betroffen dar und sollten nur in Ausnahmefällen und im Einklang mit geltendem Recht angefordert werden (z. B. notwendige Pflicht bei Erstidentifikation). Nicht benötigte Angaben (z. B. Zugangs- und Seriennummer, Nationalität, Größe, Augenfarbe, Lichtbild und maschinenlesbarer Bereich) dürfen und sollten geschwärzt werden!
- Auskunftsanfrage zur Aufzeichnung einer ***Sicherheitskamera*** (z. B. Parkplatz, Verkaufsräume) nach Art. 11 DS-GVO (Identifizierung betroffener Personen nicht erforderlich). In diesem Fall

sind der Anfrage zusätzliche Daten (Tag und Uhrzeit) einer möglichen Aufnahme hinzuzufügen. In einem, vor dem AG Pankow[67] verhandelt Fall ging es um ***Videoaufnahmen in einer S-Bahn***. Trotz konkreter Angaben, wurde eine Auskunft (Videomaterial) wegen Verletzung der Rechte Dritte (auf dem Video), nicht erforderlicher Identifizierung und einem unverhältnismäßig hohen Aufwand abgelehnt und dies im Urteil bestätigt.

- Unter ***Bewerbungsunterlagen*** fallen auch interner Notizen mit Personenbezug (z. B. auf Unterlagen oder zum Gespräch, ob digital oder auf Papier u.ä.). Kein Recht besteht auf die Information zum Entscheidungsprozess oder Vergleichsunterlagen von Mitbewerbern gem. Entscheidung BAG (8 AZR 287/08) und des EuGH (C-415/10).

(3) Zur (IT-) Datensicherheit

(a) BKA Bundelagebild Cybercrime 2021[68]

Der Bundeslagebild Cybercrime des Bundekriminalamtes (BKA) für 2021 ist veröffentlicht, eine spannende Lektüre. „*2021 war geprägt von Angriffen auf kritische Infrastrukturen, die öffentliche Verwaltung oder internationale Lieferketten. Neben monetären Schäden beeinträchtigen derartige Angriffe auch die Funktionsfähigkeit des Gemeinwesens. Ransomware war erneut die primäre, gesamtgesellschaftliche Bedrohung im Bereich der Cybercrime. Das Bedrohungs- und Schadenspotenzial ist im Jahr 2021 nochmals spürbar angestiegen.*“ Die Anzahl der Cyberstraftaten ist um 12% gestiegen, die Aufklärungsquote liegt bei ca. 30% und der Schaden alleine aus Ransomware bei ca. 24,3 Mrd. €. Fatal lesen sich die Modi Operandi:

- ✖ Erpressung *2: Standard Modus mit Verschlüsselung und Veröffentlichung.
- ✖ Erpressung *3: Zusätzliche DDoS Attacken um Server beim Opfer lahmzulegen.
- ✖ Erpressung x^2: Kunden / Lieferanten der Opfer werden auch erpresst und/oder angegriffen.
- ▣ Grundsätzlich kann jeder Ziel von Angriffen sein. Schwerpunkt in 2021 waren die Branchen verarbeitendes Gewerbe, Finanzsektor, Einzelhandel sowie öffentliche Einrichtungen.

(4) Zu angrenzenden Themen

(a) Warnungen kurz notiert

i) BKA warnt …[69]

vor betrügerischen E-Mails, die vermeintlich vom BKA selbst oder von Polizeibehörden stammten.

ii) BSI warnt …[70]

vor Spoofing (falsche Telefonnummernanzeige) mit BSI - Rufnummer

iii) t3n warnt …[71]

vor Alex, Siri, Cortana & Co im Home-Office wegen mithören von Betreibsinternas

iv) WDR (mobile.de) warnt …[72]

vor Apotheken – Apps, die personenbezogene Daten in großem Umfang weiterverkaufen

(b) Google-Fonts, nettes Mahnschreiben

Mehrfach, unter anderem beim Datenschutz-Guru und der Datenschutz Nord Gruppe[73], wird von einem netten Schreiben an viele Websitebetreiber mit Google-Fonts Nutzung berichtet und mit Verweis auf ein Urteil des Landgerichts München (Az. 3 O 17493/20) um Überweisung von 100,00€ Schadenersatz gebeten, um aufwendige Verfahren gleich zu vermeiden. Empfehlung: 1.) Speichern Sie die Google-Fonts lokal, dann wird auch keine IP-Adresse (personenbezogene Daten) übermittelt. 2.) Wägen Sie ab bzw. holen Sie sich Rechtsberatung ob Sie darauf eingehen wollen oder nicht.

(c) Hilfreich

BSI Hilfestellung zum Kinderschutz: „Smarte Geräte für Kinder ja, aber mit Schutzmaßnahmen, Gespräche, Technickgestaltung[74]“.

(1) 🖂 ➔ **07@2022**

(a) Stärkung der Verbraucherrechte

i) „Der Kündigungsbutton“

Wie auf der Seite des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) veröffentlicht[75], kommt der Kündigungsbutton bzw. muss kommen! (BGB § 320k) Gesetz ist seit 01.07.2022, dass bei abgeschlossenen, zu bezahlenden Dauerabonnements, ob Handy, Streaming, Zeitungen, Fitness usw., unabhängig vom Abschlussdatum und der Ursprungsform, auf der Website eine Kündigungsbutton in gleich – guter Sichtbarkeit wie der Abschlussbutton vorhanden sein muss. Die Kündigung sollte mit zwei Klicks abgeschlossen und vom Unternehmen umgehend bestätigt werden. Ohne Datumsangabe gilt der früheste Kündigungstermin.

ii) Klagen von Verbraucherverbänden rechtens

In einem Verfahren zur Klage der Verbraucherzentrale Bundesverband gegen Meta/Facebook hatte der BGH wegen Zweifel an der Gültigkeit der Klage, korrekterweise den EuGH um Entscheidung gebeten. Mit Urteil C-319/20[76] vom 28.04.2022 hält der EuGH fest, dass die Klage eines Verbandes ohne Auftrag und ohne konkrete Verletzung:

„nichts entgegensteht, sofern die betreffende Datenverarbeitung die Rechte identifizierter oder identifizierbarer natürlicher Personen aus dieser Verordnung beeinträchtigen kann“.

Die Frage der TRANSPARENZ gegenüber dem Verbraucher, insbesondere die Einwilligung, dürfte für Verbraucherschützer im Fokus stehen. Ist der Verbraucher verständlich und vollumfänglich über die erhobenen Daten, den Zweck und die Verarbeitung informiert und hat genau dazu seine Einwilligung gegeben?

iii) „Die UPDATE – Pflicht“

Bereits zum 01.01.2022 ist der BGB § 327f Aktualisierungen in Kraft. Darin lautet es in Absatz (1):

„Der Unternehmer hat sicherzustellen, dass dem Verbraucher während des maßgeblichen Zeitraums Aktualisierungen, die für den Erhalt der Vertragsmäßigkeit des digitalen Produkts erforderlich sind, bereitgestellt werden und der Verbraucher über diese Aktualisierungen informiert wird. Zu den erforderlichen Aktualisierungen gehören auch Sicherheitsaktualisierungen.“

Ziel sind vor allem Anbieter von IoT / Smart - Home Geräten, da nach Bericht der IoT – Security – Foundation aus November 2021[77] hier die Lage völlig inakzeptabel ist. 80 % aller Vertriebsfirmen von IoT – Geräten reagieren gar nicht oder nur unzureichend auf gemeldete Sicherheitslücken, zumal diese es nicht schaffen, einfachste Maßnahmen wie ein Meldesystem zu implementieren. Dabei wurde die Strategie in Form der Konzeption und Regelwerke analysiert und noch nicht einmal die Geräte selbst. Eine „Ampel – Liste“ zur Einordnung der Hersteller befindet sich auf Seite 20ff des Berichts.

(b) Anbieter von Videokonferenzen nicht mehr Auftragsverarbeiter

Laut 27. Datenschutzbericht 2022 der Landesbeauftragten für Datenschutz und die Informationsfreiheit NRW[78] (DS-GVO konform: JA, aber kein Auftragsverarbeitungsvertrag mehr notwendig):

*„Auch Videokonferenzdienste, die bis zum 1. Dezember 2021 als Telemediendienste eingeordnet wurden, sind nunmehr als Telekommunikationsdienste zu bewerten. Das führt unter anderem dazu, dass Stellen, die Videokonferenzdienste einsetzen, keinen Auftragsverarbeitungsvertrag mehr mit den Videokonferenzanbieter*innen abschließen müssen und für die aufgrund der Übertragung des Videochats verarbeiteten personenbezogenen Daten nicht mehr verantwortlich sind. Selbstverständlich sind sie nach wie vor dazu verpflichtet, technische und organisatorische Maßnahmen zu treffen, wie zum Beispiel datenschutzfreundliche Grundeinstellungen vorzunehmen.“*

Das bedeutet aber auch, dass zum Setzen von Cookies grundsätzlich eine Einwilligung erforderlich ist (kein berechtigtes Interesse des Verantwortlichen). Ausnahme nach TTDSG § 25 gilt ausschließlich für zwingend notwendige Informationen zur Kommunikation (Sprache, Browser usw.).

(2) Zur (IT-) Datensicherheit

(a) Jeder 2te Angestellte umgeht Sicherheitslösungen

Die Zeitschrift für Informationssicherheit <kess>[79] berichtet von einer CISCO – Studie über die Befragung von 1.000 Angestellten. Ca. 50 % der Befragten empfinden die IT – Sicherheitslösungen zu kompliziert, umständlich und zeitraubend, mit im Durchschnitt 15 Minuten täglichem Aufwand. Um ihre Arbeit schneller zu erledigen, umgehen 55 % wöchentlich und sogar 17 % täglich die Sicherheitsmaßnahmen (*„gut gemeint oder das Gegenteil von gut“*).

Neben Information und Sensibilisierung der Mitarbeiter sollten die Sicherheitsmaßnahmen möglichst intuitiv nutzbar sein. Mittlerweile verbreitet ist die 2-Faktor-Authentifizierung über Authenticator Apps, z. B. von Sophos, Google, Microsoft, oder PhotoTAN / SMS von Banken und Online-Portalen, oder USB – Schlüssel – Keys (Infolinks – Beispiele in der Fußleister[80]).

Auf der anderen Seite zeigt die Studie, dass 38 % der Befragten ihrem Unternehmen in Bezug auf Sicherheit misstrauen. Deshalb fühlen sich 71 % mit Passwörtern wohl, 61 % noch mit Fingerabdruck und beim Gesicht – Scan nur noch 46 %. Transparenz ist da ein wichtiger Faktor.

(b) Risiko zu IIoT und OT hoch

So ein Bericht der Barracuda Network Inc.[81] zu *Industrial – Internet – of – Things* und Operational – Technology *(Marktforscherstudie mit 800 teilnehmenden Managern, Projektleitern, IT-Admins aus diversen Branchen)*.

- Mehr oder weniger als 90 % hatten in den letzten 12 Monaten einen Sicherheitsvorfall, sind ziemlich besorgt über die aktuelle Bedrohungslage und hatten mehr als einen Tag mit einer Sicherheitsverletzung zu kämpfen.
- Im verarbeitenden Gewerbe liegt die Implementierung von Sicherheitsprojekten bei lediglich 24 % und im Gesundheitsweisen bei nur 17 %. Mit Implementierung eines Sicherheitsprojektes haben 74 % davon keinerlei Auswirkung eines Vorfalls verspürt.
- Sicherheitsfokus sollte auf Konnektivität & Endgeräte, Netzwerksegmentierung, Netzwerk- & Webanwendungsfirewalls und Multi – Faktor – Authentifizierung liegen.

(3) Zu angrenzenden Themen

(a) Systemschutz schon mit wenigen Mitteln

Liest man das „Register aktueller Cyber-Gefährdungen und – Angriffsformen v2.0“ (BSI / Cyber Alliance)[82], sind es nicht die Vielzahl der Begriffe (Whaling, Maskerade, Nicknapping, Replay usw.) die etwas erschrecken, sondern die Arten der Abläufe (siehe Definitionen; „Was es alles so gibt!“).

Die SOPHOS Ltd. © (internationale Sicherheitssoftware & -support / GB) gibt in einem Whitepaper 7 einfache Tipps um die eigenen Systeme zu schützen[83].

- ✔ Multi – Faktor – Authentifizierung (MFA) zwingend für Systemadmins und Sicherheitskonsolen
- ✔ Für externe Verbindungen zwingend das Remote – Desktop – Protcol (RDP) blockieren
- ✔ Alle Endgeräte sollten geschützt sein, auch wenn sie nur Offline sind
- ✔ Vermeidung von Hacker – Zugängen durch Schulung zu Phishing (Mail, Web) oder Identitäts-diebstahl durch strenge Berechtigungs- und Passwortkonzepte (mit mind. 2-Faktor-Auth.)
- ✔ Werkzeuge / Tools für Administration streng und eng begrenzen (Skalpell statt Hammer)
- ✔ Update, Update, Update, insbesondere externe Schnittstellen
- ✔ Erstellen Sie einen Vorfallplan (Incedent Responce Plan) für den Notfall

Über den Link in der Fußleiste kann das Whitepaper mit Erläuterungen angefordert werden.

(b) Gravierende Sicherheitsmängel in mehreren Kita-Apps

… entdeckt, so ein Bericht des Spiegels[84]. Nur 12 von 42 geprüften Apps mit denen Eltern und Erzieher kommunizieren sind unbedenklich (Verschlüsselung, Cloud-Speicher, Adressen u. ä.).

(c) Datenleck Twitter

Lt. „golem.de“ will ein Hacker 5,4 Mio. Datensätze von Twitter – Usern verkaufen.[85]

(1)  ➔ **08@2022**

(2) Zum Datenschutz

(a) Whistleblower und Datenschutz

Das Bundeskabinett hat Ende Juli das Hinweisgeberschutzgesetz (HinSchG) verabschiedet. Die Beratung im Bundestag erfolgt nach Stellungnahme durch den Bundesrat.[86] Eine EU – Richtlinie existiert bereits seit 23.10.2019[87], mit verpflichtender Umsetzung in nationales Recht bis 17.12.2021, was in der vorgehenden Regierungskoalition an der CDU gescheitert ist und jetzt umgesetzt wird. Das Hinweisgeberschutzgesetz ergänzt bestehende, gesetzlichen Regelungen (Geldwäsche, Kreditwesen, Wertpapiere, Versicherung, Börse, Wirtschaftsprüfung, Marktmissbrauch, Verkehr, nationale Sicherheitsinteressen, Verschwiegenheits- und Geheimhaltungspflichten u. ä.).

i) Hinweisgeberschutzgesetz (HinSchG)

Ziel von EU-Richtlinie und Gesetz ist eine bessere Durchsetzung des Rechts in Deutschland und Europa zum Schutz von Leben, Leib, Gesundheit, Beschäftigten und / oder ihrer Vertretungsorgane. Mit den Mindeststandards soll ein hohes Schutzniveau für Personen erreicht werden, die im Zusammenhang mit ihrer beruflichen Tätigkeit (Arbeitnehmer*/innen, Beamte*/innen, Selbstständige, Anteilseigner*/innen oder Mitarbeiter*/innen von Lieferanten) Informationen über Verstöße erlangen und diese melden.

Neben externen Meldestellen beim Bundesamt für Justiz (neu und bundesländerübergreifend), der BaFin, dem Kartellamt und der Finanzämter, ist jedes Unternehmen ab 50 Mitarbeitern verpflichtet, ein unabhängiges, internes Meldesystem zu installieren (ob gemeinschaftlich bis 249 MA, im Konzern oder über externe Dritte). In engen Grenzen (§§ 32ff HinSchG) ist auch eine Veröffentlichung (Offenlegung) möglich. Schadenersatzanspruch kann durch Benachteiligung des Hinweisgebers entstehen (aber auch für unredliche Hinweisgeber, bei grob fahrlässigen, unrichtigen Meldungen). Es gilt die Umkehr der Beweislast durch den Arbeitgeber, dass kein Zusammenhang besteht. Für das interne Meldesystem bestehen Informationspflichten (Eingangsbestätigung nach 7 Tagen, Statusbericht nach spätestens 3 Monaten an den Hinweisgeber) und eine Dokumentations- bzw. Berichtspflicht. Es gilt ein Ausschluss der Verantwortlichkeit für Informationen, die zur Weiterleitung notwendig sind und einem rechtlich einwandfreiem Zugriff des/der Hinweisgeber unterlagen.

ii) Schutz der Personendaten

Das Vertraulichkeitsgebot (§§ 8, 9 HinSchG): *„Informationen über die Identität einer hinweisgebenden Person oder einer Person, die Gegenstand einer Meldung ist, sollen nur in Ausnahmefällen herausgegeben werden dürfen, etwa in Strafverfahren auf Verlangen der Strafverfolgungsbehörden.(Gesetzliche Ausnahmen: Straf- und Bußgeldverfahren, gerichtliche Entscheidungen, BaFin, Bundeskartellamt, bei Erforderlichkeit zur Ergreifung von Folgemaßnahmen und bei Einwilligung).“*

iii) … im Datenschutz

Eine gute Vorlage ist die Orientierungshilfe zu Whistleblower-Hotlines der Datenschutzkonferenz der Aufsichtsbehörden (DSK) aus Ende 2018[88]. Zur Einordnung nach den Vorschriften zum Verzeichnis der Verarbeitungstätigkeiten (Erläuterung Fußnote[89]):

- ***Grund, Art, Zweck der Verarbeitung:***

  Beschäftigte in der Organisation nehmen Missstände oftmals als erste wahr und können durch ihre Hinweise dafür sorgen, dass Rechtsverstöße aufgedeckt, untersucht, verfolgt und unterbunden werden. Für diese Verantwortung verdienen sie Schutz vor Benachteiligungen (Repressalien), die ihnen wegen ihrer Meldung drohen oder sie davon abschrecken können.

- ***Zugriff, wer verarbeitet die Daten:***

  Nur unabhängige, mit der Aufgabe betraute fachkundige Mitarbeiter* (§ 15 HinSchG; Liste).

- ***Betroffene Personen und personenbezogene Daten (-Kategorien):***

  Alle natürlichen Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld der beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese melden.

- ***Rechtsgrundlage, Löschfristen, Besonderheiten:***

Eine rechtliche Verpflichtung nach dem HinSchG (Art.6 Abs.1c DSGVO) besteht zur Datenlöschung nach der regelmäßigen Verjährungsfrist von 3 Jahren (§ 195 BGB mit Besonderheiten zu Empfängern, Transfer, Drittland)

Schutzkonzept:

Aufgrund des hohen Schadenspotentials für den Betroffenen sind zum bestehenden Schutzkonzept (TOM) umfangreiche Schutzmaßnahmen zur deutlichen Reduzierung der Eintrittswahrscheinlichkeit getroffen (z. B. strenges Berechtigungskonzept, separate, Systemumgebung, 2FA, Pseudonymisierung / Anonymisierung u. ä.).

PS: Das Schutzkonzept sollte die Eintrittswahrscheinlichkeit deutlich reduzieren. Bei unverändert hohem Risiko (Schadenpotential x Eintrittswahrscheinlichkeit) ist eine Vorstellung bei der Aufsichtsbehörde vorab vorzunehmen (Art.36 DS-GVO; zur Risikoabwägung siehe Fußnote[90], Zusammenfassung SDM, Seite 7).

(b) Werber & Adresshändler gemeinsam verantwortlich

Die Aufsichtsbehörde (LfDI) Rheinland – Pfalz stellt in Ihrem Tätigkeitsbericht 2020 die gemeinsame Verantwortlichkeit von Werbenden und Adresshändlern fest, *„da das werbende Unternehmen nicht selbst über die personenbezogen Daten“* verfügt. (Seite 35 Punkt: 5.3)[91]

(3) Zur (IT-) Datensicherheit

(a) Multi-Faktor-Authentifizierung wirkt!

Schützen Sie alle (mindestens wichtigen) Anwendungen und Apps mit einer Multi-Faktor-Authentifizierung (MFA, z.B. Benutzer/Passwort + Authenticator auf Zweitgerät), es wirkt. Ein Bericht von Europol zeigt, dass die Multi-Faktor-Authentifizierung (MFA) Cyberattacken effektiv abwehren kann. Im konkreten Fall gaben die Hacker angesichts der MFA ihren Ransomware-Angriff einfach auf, so it-daily.net.[92] (BSI erklärt 2 Faktor Authentifizierung)

(b) Cloud, einfach verschlüsselt und synchronisiert

Wie einfach (und günstig) eine Ende – zu – Ende Verschlüsselung in der Cloud mit einem Austausch zwischen verschieden Geräten / Standorten funktionieren kann ist auf golem.de nachzulesen[93]. Mit der Verschlüsselungssoftware liegen die Daten verschlüsselt in der Cloud. Zum Bearbeiten wird eine virtuelles, unverschlüsseltes Laufwerk auf dem eigenen Gerät erzeugt. Schließt man das virtuelle Laufwerk, werden die Daten verschlüsselt und in der Cloud abgelegt. Eine Anleitung zum Nachlesen.

(4) Zu angrenzenden Themen

(a) Projekt „No More Ransom“ ohne Zahlung entriegeln

Wir alle wissen, je mehr Lösegeld gezahlt wird, desto attraktiver ist ein Angriff für Kriminelle. Mit dem Angebot des Projektes „NoMoreRansom“[94] konnten mehr als 1,5 Millionen Opfern geholfen werden. Dadurch wurden Lösegeldzahlungen in Höhe von ca. € 1,5 Milliarden verhindert (ZDNET).[95]

(b) Zweifel? Phishing Mail

Die Verbraucherzentrale NRW veröffentlicht aktuell im Umlauf befindliche Betrugsmails und nimmt zur Prüfung verdächtige E-Mails an und veröffentlicht diese bei Betrugsversuch.[96]

(c) Wichtiges Update Apple Produkte!

Apple warnt vor schweren Sicherheitslücken bei iPhones, iPads und Macs: Laut Apple könnten Hacker die volle Kontrolle über die Geräte erlangen. Sicherheitsexperten empfehlen ein umgehendes Update.[97] In verschiedenen Beiträge wird berichtet, dass die Auto-Update-Funktion hier nicht greift und das Update unverzüglich vorzunehmen ist (Apple-Anleitung). Deshalb habe ich den Hinweis hier aufgenommen.

(1)  ➔ **09@2022**

(2) Zum Datenschutz

(a) Aufsicht prüft Absicherung von E-Mail-Accounts[98]

Zur eigenen Absicherung lohnt es für Verantwortliche, sich mit dem Thema auseinander zu setzen, auch wenn die Prüfung zunächst nur stichprobenartig durch die Aufsicht in Bayern erfolgt. Aufgrund ihrer Befugnisse nach Art. 58 DS-GVO nimmt die Aufsicht eine Präventionsprüfung vor.

„Seit mehreren Monaten können wir ein verstärktes Aufkommen von Cyberattacken auf E-Mail-Accounts von Verantwortlichen … Die eigentlichen Ursachen solcher Cyberangriffe sind nicht selten in einer unsachgemäßen Bedienung (u. a. aufgrund mangelndem Sicherheitsbewusstsein bei den Beschäftigten) oder in einer fehlerhaften Konfiguration und Absicherung der E-Mail-Accounts … Diesen kann jedoch aktiv mit vertretbarem Aufwand entgegengewirkt werden, um die drohenden hohen Schäden – wirtschaftlich wie datenschutzrechtlich – … gering zu halten oder im Idealfall ganz zu vermeiden.“

i) Der Antwortbogen[99]

… enthält fünf Aussagen, die mit „Ja“ oder „Nein, nicht / teilweise (Begründung ist beizufügen)“ zu beantworten sind (Kurzform):

1. Phising – Awerness und allgmeines Sicherheitsbewusstsein

   Werden Mitarbeiter/-innen regelmäßig und passend zu öffentlich bekannten Bedrohungslagen und E-Mail – Angriffsarten in geeigneter Weise geschult?

2. Passwörter, Mehr – Faktor – Authentifizierung und Benutzerverwaltung

   Besteht ein Rollen- und Berechtigungskonzept nach dem Erforderlichkeitsprinzip, Zugangspasswörter mit ausreichender Komplexität und besonders schützenswerte Bereiche mit Mehr – Faktor – Authentifizierung bei regelmäßiger Rechteüberprüfung?

3. Administrative Pflege und Konfiguration der E – Mail – Konten

   Erfolgt die Verwaltung der Postfächer in strukturierter Form durch eine Fachkraft / -abteilung / Dienstleister? Sind die Einstellungen gezielt konfiguriert, abgesichert und werden regelmäßig überprüft (Änderung „Default“)? Werden Sicherheitseinstellung für Weiterleitung, Abwesenheit und Onlinezugang berücksichtigt?

4. Überprüfung Datenverkehr

   Werden Aktivitäten auf bekannte, schadhafte Zugriffe kontrolliert, blockiert und sind mit Alarmhinweis versehen? Besteht ein Protokollierungs- und Analysekonzept (Umgang mit Störungsmeldungen, Manipulationsschutz u.s.w.)?

5. Device und Patch Management sowie Backup – Konzept

   Besteht eine Inventarübersicht aller IT-Komponenten und eingesetzter Software mit Sicherheitsvorgaben zu Einstellungen und Verwendung? Besteht ein Update und Backup – Konzept mit regelmäßiger Überprüfung?

ii) Detaillierte Checkliste (Handreichung)[100]

Zu den 5 Fragen werden konkrete Detail – Punkte zur Selbsteinschätzung angeführt (☐/☒).

iii) Informationsblatt[101]

(b) E – Mail – Stress

Folgt man einer Studie von SEPPMail[102] fühlt sich jeder 4. ab 29 E – Mails pro Tag gestresst und ich kenne viele, deren tägliche Mails diese Grenze weit übersteigen. Da gibt es die Gruppe der Autarken (Wichtig: Sicherheit, Manipulationsschutz) und die der Agilen (Wichtig: Erreichbarkeit, Schnelligkeit) mit unterschiedlichem Stress- und Vorsichtlevel, denn:

Je gebildeter Menschen in Sachen Cyber Security sind, desto besorgter: 60 % der geschulten MitarbeiterInnen sind aufgrund ihrer Kompetenz gestresst – weil sie die zahlreichen Angriffsoptionen kennen.

Mögliche Gegenmaßnahmen:

- ★ Zumindest die eigenen E – Mails sollten einen aussagefähigen Betreff enthalten (INFO / AUFTRAG / NACHFRAGE / NACHTRAG u.s.w.)
- ★ Im ersten, auf dem Bildschirm abgebildeten Absatz sollte Anlass und Auftrag ersichtlich sein. Empfänger in <cc> = „kann man lesen, oder später, oder aber muss man nicht“.
- ★ Sensibilisierungsschulungen sind wichtig (und nicht nur vorgeschrieben).

- Erläuterung der Sicherheitsvorkehrungen (Firewall, Spam – Filter, Blacklists, Sperrungen, Absenderkontrollen u. ä.) reduziert das Stresslevel und gibt Sicherheit.
- Jederzeitige, freundliche Hilfestellung bei Zweifeln und Störungsfällen.
- E – Mail Signaturen, Verschlüsselungen oder eine Verlagerung von wichtiger Kommunikation auf „END TO END“ verschlüsselte Messanger.
- Und natürlich die Grundprinzipen: „Weniger ist mehr!“; „Fasse Dich kurz und eindeutig!“.

(3) Zur (IT-) Datensicherheit

(a) Mit Verantwortung am Arbeitsplatz:

- ist der Anwendungszugriff bei Abwesenheit zu sperren,
- sind Dokumente, insbesondere sensible Dokument, immer wegzuschließen und auf keinen Fall in der Öffentlichkeit zu bearbeiten,
- sind Passwörter nie unter, neben oder auf dem Schreibtisch / Monitor zu platzieren und auf keinen Fall an Dritte weiterzugeben,
- sind E-Mails stets kritisch auf Seriosität zu prüfen,
- sind öffentliche WLAN – Netze zu meiden,
- sind Unregelmäßigkeiten oder Hardwareverlust umgehend zu melden,
- und sich bei Fragen oder Unsicherheiten an die betrieblich Verantwortlichen zu wenden.

Warum? Siehe nachfolgenden Punkt 4(a).

(b) MS Windows 10 Support endet(!)

Ich musste mir erst die Augen reiben, war nicht zur Veröffentlichung für Windows 10 die „endgültige“ Betriebsversion angekündigt? Es scheint nicht so zu sein! Bei Home und Pro (Privat) in der Version 21H1 enden Updates am 13.12.2022 (dieses Jahr), bei 21H2 am 13.06.2023, bzw. Enterprise and Education (21H2) am 11.06.2024. Wer auf die Version 22H2 (z.B. im Rahmen des Windows – Insider – Programms aktualisiert hat, kann mit Updates bis 14.10.2025 rechnen.[103] Hilfreich ist sicherlich die eigene Version zu prüfen mit <⊞> + <R> und Eingabe <winver>[104]

(4) Zu angrenzenden Themen

(a) Wer haftet den nun?

Wer kann bei einem Datenschutzverstoß überhaupt in Anspruch genommen werden? Diese Frage taucht in Regelmäßigkeit immer wieder auf. Zitiert werden i. d. R. die Urteile des OLG Dresden vom 30.11.2021 (AZ.: 4 U 1158/21)[105], BAG v. 05.02.2004 (AZ:8 AZR 91/03)[106] und LAG Sachsen vom 07.04.2022 (AZ: 9Sa250/21)[107]

i) Geschäftsführer / Unternehmen

Grundsätzlich haften die Verantwortlichen, die alleine oder gemeinsam über Zweck und Mittel der Verarbeitung (und deren Erhebung) personenbezogener Daten entscheiden (Art.4, Nr.7 DS-GVO). Das sind i. d. R. Geschäftsführer, Vorstände u.s.w. Nach der Entscheidung des OLG reicht es aus, von der Datenverarbeitung zu profitieren, sie zu veranlassen oder zu dulden, ohne selbst Zugriff auf, oder Verarbeitung von Daten zu haben. Im Normalfall übernimmt das Unternehmen das Bußgeld / den Schaden. Bei Missachtung des Datenschutzes / -sicherheit können auch die Verantwortlichen wegen mangelnder Organisation / Aufsichtspflicht persönlich haften.

ii) Mitarbeiter

Das Bundesarbeitsgericht unterteilt die Mitarbeiterhaftung in leichte Fahrlässigkeit ohne Haftungsfolgen (bei leichten Pflichtverstößen, Fehler können passieren), mittlere Fahrlässigkeit mit einer anteiligen Haftung (Mitarbeiter hätte Schaden voraussehen können) und grobe Fahrlässigkeit (wissentlich Schaden oder Regelverletzung in kauf genommen) mit voller Haftung bei sozialen Grenzen.

Im Fall des OLG Dresden wurde trotz mehrfachen Hinweises auf den Verstoß gegen die Informationssicherheitsrichtlinie (Clean-Desk) verstoßen, was zu einer erheblichen Pflichtverletzung führte und nach Mahnungen und Abmahnung, folgte die (rechtmäßige) Kündigung.

(1) 🕮 ➔ **10@2022**

(2) Zum Datenschutz

(a) „Drittlandtransfer, ungelöst, wieder in aller Öffentlichkeit! - Kurz mal durchgelüftet“

Wie war das nochmal?

i) Schrems II Urteil

Über Datenschutzkreise hinaus sehr gut bekannt ist das (sogenannte) Schrems II Urteil des EuGH vom 16. Juli 2020 (C-311/18)[108]. Zu den Auswirkungen hat der Bundesbeauftragte (BfDI)[109] in einer 3-seitigen Stellungnahme Position bezogen und dazu ein „Prüfschema Drittstaatentransfers“ veröffentlicht[110].

ii) US-Datenrecht

Übrigens, die wissenschaftlichen Dienste des Deutschen Bundestages haben auf Anfrage aus dem Bundestag eine Stellungnahme / Dokumentation zum US-Datenrecht aus deutscher Datenschutzsicht erstellt[111]. Sehr interessante und übersichtliche Ausführungen zum Thema.

iii) Aufsicht weitet Prüfung aus

Das Handelsblatt berichtete unter dem 13. April 2021[112] von Ausweitungen der Prüfung durch Aufsichtsbehörden, u. a. zur US – Cloud - Nutzung.

iv) Was ist mit Großbritannien?

Wie haufe-online im August 2021 berichtete[113], gibt es für Großbritannien einen Angemessenheitsbeschluss der EU, der aber nach 4 Jahren überprüft werden muss. Wenn die Briten allerdings, wie vorgesehen, sich durch eine Reformierung von der DS-GVO trennen wollen, kann dieser auch früher hinfällig werden und Großbritannien gilt dann als Drittland, was im Auge zu behalten ist.

v) Die laufende Abmahnwelle

Dann war und ist da noch die aktuelle Welle der Abmahnungen wegen Einbindung von „google-fonts“ in die eigene Website. Eine Vielzahl der Kommentierungen sieht eine Unrechtmäßigkeit wegen notwendiger Übermittlung der IP-Adresse darin, man sollte aber nicht zahlen (i.d.R. zwischen 100€ bis 200€). Jedoch sind die „google-fonts“ sofort lokal einzubinden, oder gleich eigene Schriftarten einbinden (z.B. siehe Fußnote[114]).

vi) Neues US-Dekret zum Datenschutz

Aktuell – unter vielen anderen – berichtet die tageschau am 7. Oktober 2022 zum Vorstoß des US-Präsidenten mit einem neuen Dekret zum Datenschutzabkommen[115].

vii) Vorsichtiges Fazit:

Bis der Beschluss zum Dekret und ein mögliches, neues Privacy Shield besteht, wird es noch Monate dauern. Ob das Privacy Shield dann vor dem EuGH Bestand hat, muss sich erst noch zeigen. Max Schrems steht bereits in den Startlöchern und sieht einen Verstoß gegen die EU Grundrechtecharta. Es sieht eher nach eine Verschnaufpause als nach einer Lösung aus. Zwei Hinweise noch:

- Fernzugriff aus einem Drittland (z. B. Support) und / oder Speicherung in einer Cloud außerhalb der EU ist immer als Übermittlung anzusehen (Europan Data Protection Supervisor).
- Auch nur bei der Durchleitung über ein Land mit nicht angemessenem Schutzniveau, ist die Einhaltung der Sicherheit von personenbezogenen Daten zu gewährleisten.

(b) Info & kurze Checkliste zu Drittlandtransfer (10/2022)

[LINK] … einschließlich Erläuterungen zu ggf. erforderlichen, „zusätzlichen Maßnahmen“ des European Data Protection Board (edpb).

(3) Zu Datensicherheit

(a) Cyberangriffe können jeden treffen

Ob Studien vom IT-Branchenverband Bitkom[116], PWC, dem jährlichen Lagebericht des Bundesamtes für Informationssicherheit[117] (den hat übrigens schon der Vize Dr. Schabhüser

gezeichnet), oder einfach nur der allgemeinen Presse ist zu entnehmen, die Sicherheitslage in Deutschland ist angespannt bis kritisch. Durch die Verfeinerung der kriminellen Wertschöpfungsketten (117 Millionen neue Schadprogramme in diesem Jahr) kann es heute so gut wie jeden Treffen. Beflügelt werden die Angriffe durch die starke Zunahme des Homeoffice, möglichst noch mit privaten Geräten (BYOD), aber auch durch teilweise noch im Einsatz befindliche, alte Systeme in der Industrie.

(b) Noch mal Homeoffice

Auch für den Heimarbeitsplatz sind Verhaltensregeln, wie organisatorische Anweisungen und technische Schutzmaßnahmen zu beachten, die in einer Richtlinie festgehalten werden sollten und ggf. mit einem Betriebsrat abzustimmen sind. Ein erstes Muster finden Sie hier [LINK] und sollte individuell angepasst werden. Die wichtigsten Punkte:

- ✔ Keine Kenntnisnahme Dritter von Gesprächen, Unterlagen, Zugriffsberechtigungen u. ä. Ein abschließbares Arbeitszimmer, mindestens verschließbare Schränke wären hilfreich.
- ✔ Möglichst ein, vom Arbeitgeber sicher konfigurierte Rechner, bzw. die Einhaltung entsprechender Sicherheitsstandards (aktueller Virenschutz, Firewall, Verschlüsselungssoftware u. ä.), was zu überprüfen wäre. Datenspeicherung nur auf Firmennetzwerk oder -datenträgern.
- ✔ Eindeutige Trennung von beruflicher und privater Verarbeitung, möglichst über getrennte Endgeräte oder einer softwarebasierten (z. B. Container-) Lösung. Keine Weiterleitung von beruflichen E-Mails an privat Mailadressen.
- ✔ Bei LAN/WLAN dürfte es hpts. über den privaten Router gehen. Neben einer sicheren Passwortverschlüsselung bieten sich getrennte Netze und ein MAC-Filter an. Zusätzlich sollte das Firmennetzwerk nur über eine zusätzlich gesicherte VPN-Verbindung erreichbar sein.
- ✔ Die Datenschutzregeln sind entsprechend auch zu Hause einzuhalten!
- ✔ Sicher sind Ihre Mitarbeiter auch in Datensicherheit und Datenschutz geschult und bei Unsicherheit oder Datenpannen steht das Unternehmen hilfreich zur Seite. Schützen Sie Ihrer Mitarbeiter, aber vermeiden Sie übergriffige Kontrollmaßnahmen.

(4) Zu angrenzenden Themen

(a) Informationsflut stresst Mitarbeiter

IT-Business berichtet[118], dass Deutsche Arbeitnehmer gestresst und überlastet sind. Dazu führen einer Operntext-Umfrage zufolge verschiedene Faktoren, wie der konstante Fluss von Daten über verschiedene Geräte hinweg, die allgegenwärtigen sozialen Medien oder die zunehmende Anzahl von Anwendungen, denen Arbeitnehmer im Arbeitsalltag ausgesetzt sind. Wegen genau dieser Informationsflut fühlen sich 82 Prozent der Deutschen gestresst.

(b) Gefährliche Zwangs-Apps für Fußballfans

Die Fußball-WM in Katar ist ohnehin problematisch. Nun müssen sich Fußball-Fans darauf gefasst machen, mit Handy-Apps überwacht zu werden so Netzpolitik.org[119].

Sorgen bereitet einerseits die App: „Ehteraz“, die Infektionen mit dem Coronavirus nachverfolgen soll. Einmal installiert, kann sie u. a. auf sämtliche Daten auf dem Handy zugreifen, WLAN- oder Bluetooth-Verbindungen überwachen, den genauen Standort auslesen und speichert auf einer zentralen Datenbank. Die andere App: „Hayya“, ist die offizielle App für die Weltmeisterschaft zur Verwaltung der Veranstaltungen. Weniger invasiv, greift aber dafür kritische Daten ab und kann u.a. den Standort auslesen, das Smartphone am Einschlafen hindern und Netzwerkverbindungen überwachen. Ferner sei sie in der Lage, persönliche Informationen „beinahe ohne Einschränkungen“ weiterzugeben.

Einige erinnern sich vielleicht noch dazu an den Einsatz der Spionage-Software „Pegasus“[120] der Geheimdienste. Besser ein billiges „Einmal-Smartphone“ mitnehmen, sicher ist sicher!

(1) 11@2022

(2) Zum Datenschutz

(a) Pflicht zur Benennung eines Datenschutzbeauftragten

i) Grundsätzlich:

Die Verantwortung, also in der Pflicht zur Einhaltung des Datenschutzes sind und bleiben immer die Verantwortlichen. Den Datenschutzbeauftragten obliegen (Art.39 DS-GVO) die Unterrichtung und Beratung der Verantwortlichen (einschl. Auftragsverarbeiter) und der Beschäftigten zur Einhaltung der Vorschriften (Abs.1a), deren Überwachung, der Zuweisung von Zuständigkeiten, sowie Sensibilisierung und Schulung (Abs.1b), der Beratung auf Anfrage bei Durchführung einer Datenschutz – Folgenabschätzung (Abs.1c), die Zusammenarbeit mit Aufsichtsbehörden (Abs.1d) und deren Anlaufstelle bei Fragen oder notwendigen Konsultationen. Dabei sind sie vollumfänglich von den Verantwortlichen zu unterstützen, zu informieren und frühzeitig einzuschalten (Art.38 DS-GVO).

ii) Die Pflicht zur Benennung:

Die DS-GVO enthält verschiedene Öffnungsklauseln für die Regelungen in einzelnen Mitgliedsstaaten zu Präzisierung des Art.37 DS-GVO und Klarstellung: §38 BDSG, Datenschutzbeauftragte für nicht öffentliche Stellen. Die Pflicht zur Benennung besteht:

- Wenn mindestens 20 Mitarbeiter ständig (auch nur am Rande) mit der automatisierten Bearbeitung personenbezogener Daten beschäftigt sind.

oder
- Wenn für die Bearbeitung eine Datenschutz – Folgenabschätzung* notwendig ist.

**) Art. 35 DSGVO bei hohem Risiko, insbesondere Art.9 besondere Kategorien, Art.10 Straftatbestände, systematische und umfassende Bewertung persönlicher Aspekte, automatisierte Verarbeitung und Profiling*

oder
- Wenn personenbezogene Daten (auch anonymisiert) übermittelt werden.

oder
- Wenn personenbezogene Daten für Markt- oder Meinungsforschung verarbeitet werden.

oder
- Bei Behörden, mit Ausnahme von Gerichten

oder
- Die Kerntätigkeit liegt in umfangreicher, regelmäßiger und systematischer Überwachung betroffener Personen (z. B. Auskunfteien, Personalabteilung, Sport- / Navigationsapps)

oder
- Die Kerntätigkeit liegt in der umfangreichen Verarbeitung von besonderen Kategorien (Art.9 DS-GVO) oder strafrechtlicher Daten (Art.10 DS-GVO). (z. B. ist eine einzelne Arztpraxis ausgenommen, eine Praxisgemeinschaft ggf. mit Labor nicht).

iii) Fragen schadet nicht:

Ob die Benennung eines Datenschutzbeauftragten notwendig ist, oder nicht, oder ein unsicherer Punkt zu klären ist, kann die Frage an einen oder Ihren Datenschutzbeauftragten nicht schaden.

(3) Zur Datensicherheit

(a) Sicherheit mit Bordmitteln

Wer keinen Informationssicherheitsbeauftragter (ISB) beschäftigt, kann oft mit nur wenigen, einfachen Maßnahmen einen größeren Schaden verhindern.

i) Cloud

In einer Studie der Cloud Security Alliance (.org; CSA)[121] gibt es nach wie vor große Bedenken gegenüber der Cloud-Sicherheit. 62% der 1.662 Befragten gehen davon aus, dass ihre Organisation / Unternehmen im nächsten Jahr von einer Datenschutzverletzung betroffen sein wird. Die meist genutzten Clouds sind OneDrive (Microsoft) und Google Drive. Zur sicheren Übertragung wird bei beiden Anbietern eine SSL-Verschlüsselung mit AES-256 genutzt, um vor dem Zugriff Dritter zu schützen. Nach dem Praxistipp des Spiegels nebst Erläuterung[122], eine der sichersten Verschlüsselungsmethoden („Goldstandard“). Für einen Zugriff wird man am Passwort des/der Nutzer* nicht vorbeikommen. Allerdings liegen die Daten auf den Servern der Anbieter unverschlüsselt. Sicherheit mit Bordmitteln:

- Zunächst ein sicheres Passwort auswählen.

- Zwei-Fakor-Authentifizierung aktiveren über z. B. Microsoft u/o Google Authenticator, oder Drittanbieter wie Sophos-Intercept-X for Mobile[123] für alle die darauf zugreifen dürfen. *(Kein Sponsoring, Werbung o. ä., nur Beispiel)*
- Und ganz sicher vor dem Zugriff Dritter ist, die Daten vor der Übertragung selbst zu verschlüsseln, z. B. mit der Open-Source-Software Cryptomator. Für Teams gibt es hier auch den Cryptomator Hub, beides mit AES-256 Verschlüsselung[124]. *(Kein Sponsoring, Werbung o. ä., nur Beispiel)* DAS, entspricht auf jeden Fall auch der DS-GVO.

ii) Betriebssystem

Ob Windows, macOS, Linux, alle Systeme sind mit den Standardeinstellungen meist gut gerüstet. Ein prüfender Blick über die Sicherheitseinstellung kann aber nicht schaden, um sicherzugehen, dass nicht ein Hinderungsgrund (aus Vorinstallation, Installation, inkompatibler Treiber u. ä.) etwas nicht aktiviert ist. Am Beispiel Windows hat sich Security-Insider in einem Artikel vom 08.11.2022(+Video, Bildergalerie)[125] mit den (ausreichenden) Bordmitteln gegen Ransomware über das 3-Stufen-Modell beschäftigt.

Stufe 1: Aktiver Viren- und Mailware Scanner (First line of defense)

Stufe 2: Aktive Überwachung des Ordnerzugriffs zur Verhinderung einer Verschlüsselung

Stufe 3: Backup zur Wiederherstellung für den Notfall

„Zehn Maßnahmen zur Absicherung gegen Angriffe aus dem Internet“ hat das BSI[126] in einer übersichtlichen Broschüre zusammengestellt[127].

iii) Router / WLAN / LAN

Kurz und übersichtlich sind auch die *„Sicherheitstipps im privaten und öffentlichen WLAN“*[128], *unter anderem:*

- *Standardpasswort und Standard - Netzwerkname ändern*
- *Aktuelle Firmware und aktiver Filter der Geräte - MAC-Adressen*
- *Langes und komplexes WLAN-Passwort (20 Zeichen, groß, klein, Zahlen, Sonderzeichen)*
- *Einrichtung eines Gast – Netzwerks für unsichere Geräte und in öffentlichen Netzwerken*
- *Ist die Firewall für den Zugang über öffentliche Netzwerke eingerichtet?(!)*
- *Einschalten, nur wenn es erforderlich ist*
- *Wenn es unvermeidbar ist, Abruf von vertraulichen Informationen über VPN.*

iv) Fragen schadet nicht

Oder fragen Sie einfach ihren Techniklieferanten / IT-Dienstleister nach den eingestellten Sicherheitsfunktionen.

(4) Zu angrenzenden Themen

(a) <u>Aktuelle Betrugsmaschen häufen sich:</u>

i) Messenger - Betrug

Das LKA Niedersachsen warnt vor: *„Messenger – Betrug: Die Gefahr durch gefälschte Freunde- oder Familienkontakte“* [129]. Versuche, Messenger - Nutzer mit Nachrichten davon zu überzeugen, dass sie Freunde oder Familienangehörige seien (neue Telefonnummer). Im Anschluss wurde um Verifizierungscodes und später um Überweisungen gebeten.

ii) Datenabgleich Paypal

Das Phishing - Radar der Verbraucherzentrale warnt aktuell vor einer Forderung nach Datenabgleich der Paypal - Kundschaft um an Verifizierungsdaten zu kommen[130].

iii) Perfider DHL – Betrug

[chip.de] Kriminelle versenden Phishing-Mails an DHL – Kunden. Wegen offener Zollgebühren (€1,89) könne ein Paket nicht ausgeliefert werden. Bezahlung über eingefügten Link[131].

Bleiben Sie wachsam, mit dem 3-Punkte-Check des BSI (Absender, Betreff, Anhang/Link)[132]

(1) 🖻 ➔ **12@2022**

(2) Zum Datenschutz

(a) Datenschutzverletzung

Nach Art.33 DS-GVO muss die Verletzung zu schützender, personenbezogener Daten innerhalb von 72 Stunden durch den Verantwortlichen an die zuständige Aufsichtsbehörde gemeldet werden, wenn dies voraussichtliche zu einem Risiko für die natürlichen Personen führt. Der Auftragsverarbeiter hat dies unverzüglich an die Verantwortlichen zu melden(!).

i) „Kleine Fische" gibt es nicht

In der NZZ ist ein kurzweiliger Bericht[133] einer Gesellschaft mit 20 Mitarbeitern. Nur so viel, dank der Sicherheitslösungen kam es zu keiner Verschlüsselung, allerdings tauchten im Darknet interne Dokumente auf und es waren Daten von tausenden Kunden betroffen (Admin: „ Stresstest").

ii) Dokumentation | Meldung | Information

Eine kurze Übersicht gibt die Website der LfDI-NRW zu den Pflichten bei einer Verletzung[134].

- 🟢 Interne Dokumentationspflicht: kein bis geringes Risiko (also immer)
- 🟡 Meldepflicht an Aufsichtsbehörde: mittleres Risiko
- 🔴 Betroffenen – Information: hohes Risiko

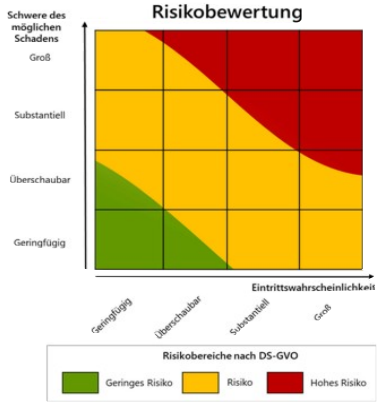
Oft genannte Beispiele für kein bis geringes Risiko sind der Verlust einer nach dem Stand der Technik verschlüsselten Festplatte, zu der ein Backup besteht, oder veröffentlichte (z.B. Telefonbuch, Website), bekannte E-Mail- oder Adressdaten u. ä.

iii) Risikoanalyse

Grundsätzlich hat eine Risikoanalyse aus Eintrittswahrscheinlichkeit und möglicher Schwere eines Schadens zu erfolgen, wie hier rechts im Bild gezeigt. Hinweis (übrigens):

„Es ist NICHT ZULÄSSIG auf Anforderungen der Grundsätze nach Art. 5 DS-GVO zu verzichten und Risiken daraus in Kauf zu nehmen. RISIKO - AKZEPTANZ oder RISIKO - TRANSFER (z. B. bekannt aus der Informationssicherheit) stehen den Verantwortlichen im Datenschutz NICHT ZUR VERFÜGUNG."

Nach Art der Daten (Adressen, E-Mail, Fotos, Benutzername, Passwort, Biometrie, Berufsgeheimnis, Standort, Bank/Kreditdaten, Gesundheit, Religion, Sexualität, Politik u. ä.) ist der mögliche Schaden für die Betroffenen einzuschätzen (Finanzieller Art, Identitätsdiebstahl, Ruf- / Image-schaden, Bloßstellung, Geheimnisoffenbarung, Existenzgefährdung u. ä.).



Bildquelle: Datenschutzkonferenz (DSK) Kurpapier Nr. 18, Schaubild Seite 5

iv) Was ist zu tun?

(a) Im Vorfeld sollte neben den Schulungen zur Sensibilisierung die Meldekette festgelegt sein, die Zusammensetzung des Notfallteams incl. Datenschutzverantwortliche, -berater und mögliche, notwendige, externe Spezialisten, sowie Kommunikationsverantwortliche.

(b) Durch technische und organisatorische Maßnahmen den Schaden analysieren, eingrenzen, abschätzen und das Risiko möglichst mindern.

(c) Geeignete Information der Mitarbeiter (einheitliches Außenbild), der Aufsichtsbehörde, der Cybereinheit der Polizei und der Betroffenen. *(Wenn die Möglichkeit besteht, dass Daten in die falschen Hände geraten könnten, sollten m. E. auch bei geringem Risiko die Betroffenen informiert werden, allein um möglich Risiken besser einzuschätzen und bevor Betroffene es aus dritter Hand erfahren.)*

v) Vorbereitung / Checkliste Schadensmeldung

Natürlich verweisen die meisten Websites der Datenschutzbeauftragten auf ihr Meldung im Online-Portal. Welche Informationen sie sich zurechtlegen sollten finden Sie auf meinem PDF-Formular[135]. Einfach öffnen und ausfüllen als Vorlage, oder als Meldung per Brief / E-Mail.

(b) MS 365, jetzt wird es spannend!

Die Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder hat eine zusammenfassende Stellungnahme zu „Microsoft-Onlinedienste“ am 24.11.2022 nach 2-jähriger Prüfung und Abstimmungen mit Microsoft veröffentlicht[136].

- ✖ Schwierigkeiten bei der Rechenschaftspflicht der Verantwortlichen, mangels vollständiger Offenlegung der einzelnen Verarbeitungen.
- ✖ Die Verwendung zu eigenen Zwecken als Auftragsverarbeiter schließt die Verwendung im öffentlichen Bereich (Schulen, Behörden) aus, ein berechtigtes Interesse zählt hier nicht.
- ✖ Offenlegung auch ohne Rechtshilfeabkommen mit der EU in einem Drittland möglich.
- ✖ Löschfristen können nur zu Zwecken von Microsoft verlängert werden.
- ✖ Eingeschränkte Kontrollrechte bei der Einschaltung von Unterauftragsverarbeitern
- ✖ Neben der Übermittlung in die USA (schon sehr kritisch nach den Schrems – Urteilen des EuGH), behält sich Microsoft auch die Übermittlung an Auftragsverarbeitern in andere Drittländer generell vor.

Fazit: **Die DSK bleibt kritisch zum Einsatz von MS 365!**

Wie sich Thüringens Landesdatenschutzbeauftragter in der Süddeutschen Zeitung äußerte, kann MS365 weder in Behörden, Schulen noch der freien Wirtschaft datenschutzkonform eingesetzt werden. *„Allerdings wolle er nun zunächst herausfinden, wie stark sie in der Unternehmerschaft verbreitet ist und unter anderem mit der Industrie- und Handelskammer über die Auswirkungen des Beschlusses sprechen.“*

(3) Zur Datensicherheit

(a) Es wird schlimmer (Cybersecurity Report `23)

Nach einer Analyse von 25 Mrd. E-Mails im Zeitraum 01.10.21 bis 20.09.22 stellt der Cybersecurity Report 2023 der Hornetsecurity[137] fest: Bereits knapp 41 % der E-Mails sind unerwünscht. Phishing ist mit einem Anteil von knapp 40 % die größte Angriffsart. Bei den Dateianhängen führen Archive mit 28 %, knapp gefolgt von MS-Office-Dokumenten (Word, Excel) mit 23 %.

i) Trügerische Sicherheit von MS365

„Microsoft 365 (Markos im Standard deaktiviert) erleichtert die Freigabe von Dokumenten, jedoch bedenken Endnutzer oft die Konsequenzen für die IT-Sicherheit nicht. Hornetsecurity fand in einer Umfrage heraus, dass 25 % der Befragten entweder unsicher waren oder davon ausgingen, dass Microsoft 365 immun gegen Ransomware - Bedrohungen sei. (Zitat)

ii) „Brand Impersonation“

… oder Diebstahl mittels geklauter Identitäten. Mit auf Social-Media-Plattformen angeeigneten Informationen über Social Engineering an Unternehmensdaten zu kommen. Zitat:

„So stieg der Anteil von LinkedIn an den weltweit entdeckten Bedrohungen durch Brand Impersonation auf 22,4 %, was einem Anstieg von 3,5 % gegenüber dem Vorjahr entspricht.“

(4) Zu angrenzenden Themen

(a) Hackerangriffe auf Handys nehmen stark zu

Wie die zeit-online aus einer dpa – Meldung berichtet[138], nehmen die Hackerangriffe mit zunehmender Verbreitung von Bezahl-Apps nach einer US-Analyse (Lexis Nexis Risk Solution) stark zu. *„Die EU-Zahlungsrichtlinie PSD2 und die damit verbundene Verschärfung der Login-Vorschriften habe Online-Zahlung und Überweisungen zwar sicherer gemacht, aber nicht narrensicher.“* Beispiel sind die in Not geratenen Angehörigen, was dringend einer Überweisung bedarf u. ä.

(b) Aufpassen wie ein Luchs

Die Sicherheitsstandards sind recht hoch, auch durch die 2-Faktor-Authentifizierung u. ä. Bei den aller meisten, gelesenen „Hacks“ geht es nur noch über den „verleiteten“ Nutzer, dafür werden keine Kosten und Mühen gescheut. Also: „Aufpassen wie ein Luchs!“

Bei Bedarf, einfach mal sprechen!

ENDNOTEN NR.

1 Quelle: SDM – Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln" der DSK (23 Seiten)
2 LINK: Kurze Zusammenfassung Baustein 51: Zugriffe auf Daten, Systeme, Prozesse (1 Seite) & Richtlinienentwurf (2 S.)
3 Quelle: https://dejure.org/gesetze/SGB_V/284.html <> https://dejure.org/gesetze/SGB_V/306.html
4 Quelle: Bundesgesetzblatt Nr. 28, 8.6.2021: Datenschutz – Folgenabschätzung (DSFA) zum PDSG, PDF ab Seite 42
5 Quelle: BfDI: Pressemitteilung zu Folgen der Gesetzgebung PDSG
6 Quelle: BSI: Schutzprofile und technische Richtlinien
7 Quelle: BSI: Telematikinfrastruktur – sichere Vernetzung medizinischer Versorgung
8 Quelle: Tagesschau: „Mobilfunkbetreiber gegen Datenschützer (und Verbraucherverbände)“
9 Quelle: BSI: „Sektorstudie Gesundheit“
10 Quelle: dsb Rep. Österreich: TEILBESCHEID SPRUCH Datenschutzbeschwerde (PDF)
Dr. Datenschutz: „Google Analytics und das Datenübermittlungsproblem“
11 Quelle: Tagesschau / Plusminus: „Nutzerdaten jahrelang online“
12 Quelle: Security-Insider: „Datenpannen jenseits der Schlagzeilen“
13 Quelle: WinFuture: „Feature, nicht Trojaner: Avira und Norton installieren Krypto-Miner“
14 Quelle: Presse – Lexikon: Datenschutz: „Wie stelle ich ein berechtigtes Interesse fest?“
15 Quelle: Dr.Datenschutz: „Anforderung an eine Einwilligung“
16 Quelle: BfDI: Pressemitteilung; EDSA: Pressemitteilung
17 Quelle: Landesanstalt für Medien NRW: „Staatsverträge „Neu: Medienstaatsvertrag (MStV)“
18 Quelle: Bayerische Staatskanzlei: „LG München I, Endurteil v. 20.01.2022 – 3 O 17493/20“
19 Quellen: EuGH Pressemitteilungen: Nr. 126/11 vom 24.11.2021 und Nr. 112/16 vom 19.10.2016
20 Quelle: Chaos Computer Club: „CCC veröffentlicht Formulierungshilfe für Digitales im neuen Regierungsprogramm“
21 Quelle: IoT Security Foundation: Report 11/2021, siehe Seite 20“
22 Quelle: WDR-Mediathek: „Angeklickt: Biometrische Daten im Angebot“; Spiegel: „Gesichtserkennung …“
23 Quelle: https://appcheck.mobilsicher.de/
24 Link: Dr.Datenschutz: „Beauty Apps und Datenschutz: Wer schön sein will, muss leiden“
25 Quelle: SDZ: „Der Albtraum für die Privatsphäre: Das Programm "Clearview AI“;
26 LINK: ULD, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Tätigkeitsbericht 2022, Punkt 5.4
27 Quelle: Datenschutznotizen: „Die große Werbekampagne per Briefpost – zulässig?“
28 Quelle: Deutsche Post direkt: „Postwurfspezial: teiladdressiert werben“
29 Quelle: Zentrale zur Bekämpfung unlauteren Wettbewerbs Frankfurt am Main e. V.: „Direktmarketing“
30 Quelle: omsels.info – Der Online-Kommentar zum UWG: „f) Mutmaßliche Einwilligung“
31 Hinweis: Art. 13, 14 DS-GVO Datenerhebung direkt und bei Dritten
32 Quelle: Orientierungshilfe der Datenschutzkonferenz zur Direktwerbung
33 Quelle: Mehr zur Werbung mit E-Mail-Signatur von Dr. Datenschutz: „Wann wird eine E-Mail-Signatur zur Werbung?“
34 Quelle: Microsoft: „Ice phishing on the blockchain“; ZDNet: „Ice-Phishing bedroht Blockchain“
35 Quelle: BSI warnt vor Produkten der Security Suite von Kasparsky
36 Quelle: BfDI: „Datenschutz in sozialen Netzwerken“; „Dürfen Behörden Facebook“, „DS-Defizite Facebook“
37 Quelle: Focus: „Was Facebook alles über mich weiß, hat mich schockiert“
38 Quelle: heise-online: „Leak: Facebook hat offenbar keine Kontrolle über Nutzerdaten“
39 Quelle: t-online: „Gericht verbietet Facebook das Sammeln von Nutzerdaten“
40 Quelle: Ausführung der Landesbeauftragten für den Datenschutz & die Informationsfreiheit – NRW
41 Hinweis: „https://volkerschroer.de/DSGVO/2021.07.27.Gemeinsam.Verantwortliche.Hinweise.pdf“
42 Quelle: Faceboook: „Informationen zu Seiten-Insights“ bzw. „Controller Addendum“
43 Quelle: golem.de IT-News: „Mastodon“; wikipedia.de: Mastodon (Software)“; Knoten: „mastodon.social“; Liste der Knoten;
44 Quelle: https://de.wikipedia.org/wiki/Kollektive_Intelligenz
45 Quelle: BfDI Tätigkeitsbericht 2022, Seite 11, Punkt 3.2.3
46 Quelle: csoonline.com: „Neue Warnung des Verfassungsschutzes vor russischen Cyberattacken“
47 Quelle: Spiegel-Online: „Wenn der angebliche Microsoft-Mitarbeiter anruft“
48 Quelle: BSI Bericht zur IT -Sicherheitslage
49 Quelle: Schufa: „Scoring bei der Schufa“; golem: „Die Schufa erläutert Scoring“
50 Quelle: NRW Justiz – Online
51 Quelle: edpb: „Guidelines 3/2022 on Dark patterns in social media patform interfaces: How to recognis and avoid them“
52 Quelle: tagesschau.de: „Wie das Grundrecht auf Datenschutz entstand.“
53 Quelle: bundesverfassungsgericht.de: „Zum Urteil des Ersten Senats vom 15.12.1983“
54 Quelle: BfDI Kurzmitteilung: „Informationen zum Online-Fragebogen des Statistischen Bundesamtes zum Zensuss 2022“
55 Quelle: Bundesministerium der Justiz: „Gesetz zur Durchführung des Zensus im Jahr 2022“
56 Quelle: BverfG: „Leitsätze zum Urteil des Zweiten Senats vom 19. September 2018“
57 Quelle. zdfheute: Sind meine Zensus-Daten sicher, Herr Kelber?“
58 Quelle: BSI: Die Lager der IT-Sicherheit Deutschland (2021)
59 Quelle: BfDI: „30. Tätigkeitsbericht“
60 Quelle: „DiFü, den digitalen Führerschein erhalten“
61 Quelle: https://bigbrotherawards.de/2022/lebenswerk-irische-datenschutzbehoerde-dpc
62 Quelle: https://bigbrotherawards.de/2022/verbraucherschutz-klarna
63 Quelle: Charta der Grundrechte in der Europäischen Union Art. 8: „https://dejure.org/gesetze/GRCh/8.html“
64 Quelle: Tätigkeitsbericht 2019 Bayrisches Landesamt für Datenschutzaufsicht, Seite 36
65 Quelle: BGH, Urteil vom 28.01.2014 - VI ZR 156/13
66 Quelle: edpb: „Guidelines 01/2022 on data subject rights - Right of access“
67 Quelle: AG Pankow: 4 C 199/21 vom 28.03.2022
68 Quelle: BKA Bundelagebild Cybercrime 2021
69 Quelle: https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/220531_FakeMailsBKA.html
70 Quelle: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Spoofing_220602.html

ENDNOTEN NR.

71 Quelle: t3n: „Homeoffice: Deshalb solltet ihr vorsichtig mit Alexa, Siri und Co sein“
72 Quelle: https://www1.wdr.de/verbraucher/digital/service-computer-Datentransport-aufs-Smartphone-102.html
73 Quele: DS-Nord-Gruppe: „Google Fonts – Schreiben mit Schadensersatzforderung an Websitebetreibende verschickt“
74 Quelle: BSI: „Kinder beim sicheren Surfen unterstützen“
75 Quelle: BMUV: „Verbraucherrechte online werden gestärkt“
76 Quelle: EuGH C-319/20 vom 28.04.2022 auf InfoCuria
77 Quelle: IoT Security Foundation. „The contemporary use of vulnerability disclosure in IoT Report 4.11.2021“
78 Quelle: https://www.ldi.nrw.de/system/files/media/document/file/27_datenschutzbericht_2022_ldi_nrw.pdf
79 Quelle: <kess> „Jeder zweite Angestellte umgeht Security-Lösungen“
80 LINKS Schlüssel-Keys: „yubico.com“, „Neowave Winkeo FIDO U2F“
81 Quelle: Barracuda Networks Inc.: „The state of industrial security in 2022.“
82 Quelle: BSI/Cyber Alliance: „Register aktueller Cyber-Gefährdungen und -Angriffsformen v2.0.“
83 Quelle: Sophos: „Erhöhen Sie jetzt Ihre Cybersicherheit! 7 Tipps, wie Sie Ihr Unternehmen gegen Cyberangriffe schützen “
84 Quelle: Spiegel: „Gravierende Sicherheitsmängel in mehreren Kita-Apps entdeckt.“
85 Quelle: golem.de: „Hacker will 5,4 Millionen Twitter-Datensätze verkaufen.“
86 Quelle: BMJ Pressemitteilung: „Hinweisgeberschutzgesetz vom Kabinett beschlossen“
87 Quelle: EU: „Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019“
88 Quelle: DSK: „Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines“ (PDF)
89 Hinweis: V. Schroer: „Zusammenfassende Erläuterung zum Verzeichnis der Verarbeitungstätigkeiten“
90 Hinweis: V. Schroer: „Zusammenfassung Das Standard - Datenschutz - Modell | Management – Info“
91 Quelle: LfDI – RP: „Tätigkeitsbericht zum Datenschut 2020, Seite 35 Nr. 5.3“
92 Quelle: it-daily.net: „Multi-Faktor-Authentifizierung: Hacker geben einfach auf“; BSI erklärt 2 Faktor Authentifizierung
93 Quelle: golem.de: „Endlich ist unsere Cloud Ende-zu-Ende-verschlüsselt“
94 Link: NoMoreRansom: „Brauchen Sie Hilfe zum Entriegeln Ihres digitalen Lebens, ohne dabei Lösegeld zu zahlen*?“
95 Quelle: ZDNET: „Ransomware: 1.5 million people have got their files back without paying the gangs. Here's how“
96 Quelle: verbraucherzentrale: „Phishing-Radar: Aktuelle Warnungen“
97 Quelle: tagesschau.de: „Apple warnt vor Sicherheitslücke“
98 Quelle: LDA-Bayern: „Datenschutzprüfungen, E-Mail Account Absicherung“
99 LINK: LDA-Bayern: „Antwortbogen“
100 LINK: LDA-Bayern: „Handreichung bzw. detaillierte Checkliste“
101 LINK: LDA-Bayern: „Informationsblatt“
102 Quelle: SEPPMAIL: „E – Mail – Stress – Studie, Mensch vs. Maschine“
103 Quelle: Microsoft: „Support dates Windows 10 Home and Pro“; „Enterprise and Education“, „Releasing WIn10 Vers. 22H“
104 Quelle: Microsoft: „Welche Version des Windows Betriebssystem verwende ich?“
105 Quelle: openjur.de: „OLG Dresden, Urteil vom 30.11.2021 - 4 U 1158/21“
106 Quelle: BAG v. 05.02.2004 (AZ:8 AZR 91/03): „Grundsätze der Beschränkung der Mitarbeiterhaftung“
107 Quelle: LAG Sachsen vom 07.04.2022 (AZ: 9Sa250/21): „Verhältnismäßigkeit Nachlässigkeit – Abmahnung – Kündigung“
108 Quelle: Info Curia: „EuGH Aktenzeichen = C-311/18“
109 Quelle: BfDI: Schrems II Urteil des EuGH (Urteil v. 16. Juli 2020, C-311/18) – Kernaussagen.“
110 Quelle: BfDI: „Prüfschema Drittstaatentransfers“
111 LINK: Wissenschaftliche Dienste des deutschen Bundestages: „US-Datenrecht, Zugriff von US – Behörden“
112 Quelle: Handelsblatt: „Deutsche Firmen in der Datenschutzfall – Behörden intensivieren Ermittlungen“
113 Quelle: haufe-online: „Großbritannien will Datenschutz reformieren und sich von der DSGVO lösen“
114 LINK: anwalt.de: „Abmahnungen wegen Google Fonts“
115 Quelle: tagesschau: „Vorstoß für ein neue Datenschutzabkommen (Vereinbarung mit der EU)“
116 Quelle: CSO Deutschland: „Bitkom-Studie: 203 Mrd. Euro Schaden pro Jahr in Deutschland“
117 Quelle. BSI: „IT-Sicherheitslage spitzt sich zu, die Lage der IT-Sicherheit in Deutschland 2022“
118 Quelle: IT-Business: „Informationsflut stresst Arbeitnehmer“
119 Quelle: Netzpolitik.org: „WM in Katar, gefährliche Zwangs-Apps für Fußballfans“
120 Quelle: deutschlandfunk.de: „Spionage-Software Pegasus“
121 Quelle: CSA: „Understanding Cloud Data Security and Priorities“ (19.10.2022)
122 Quelle: Spiegel – Praxistipp: „AES-256: Bedeutet und Sicherheit der Verschlüsselung“
123 Quelle: SOPHOS: „Mobile Threat Defense for Android, iOS und ChromeOS“
124 Quelle: Cryptomator: „Hänge ein Schloss vor deine Cloud“
125 Quelle: Security-Insider: „Ransomeware-Schutz mit Windows Bordmittel“
126 Abkürzung: „BSI“ – Bundesamt für Sicherheit in der Informationstechnik
127 Quelle: BSI: „Zehn Maßnahmen zum Schutz vor Angriffen aus dem Internet (PDF)“
128 Quelle: BSI: „Sicherheitstipps im privaten und öffentlichen WLAN“
129 Quelle: LKA Niedersachsen. „Messenger-Betrug: Die Gefahr durch gefälschte Freunde- oder Familienkontakte“
130 Quelle: Verbraucherzentrale aktuelle Warnungen: „18. November 2022: Datenabgleich von Paypal-Kundschaft gefordert“
131 Quelle: chip.de: „DHL-Kunden in Gefahr: Besonders perfide Betrugsmasche im Umlauf“
132 Quelle: BSI: „Nutzen Sie die E-Mail (Messenger) wirklich sicher?“
133 Quelle: NZZ: „Die Erpressung landet im Spam-Ordner, Tausende von Kundenadressen im Darknet: Ein Kleinunternehmen gibt einen seltenen Einblick in einen Hack“
134 Quelle: LfDI-NRW: „Meldepflicht für Verantwortliche – Verletzung des Schutzes personenbezogener Daten“
135 LINK: https://volkerschroer.de/DSGVO/Schutzverletzung.Meldung.Art.33.pdf
136 Quelle: DSK: https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf
137 Quelle: Hornetsecurity: „OUT NOW: Cybersecurity Report 2023“
138 Quelle: Zeit-Online: „Cyber-Report: Hackerangriffe auf Handys nehmen stark zu“