Übersicht 2021 | Zum Datenschutz aufgefallen

Information zum (Weblink)

Datenschutz - Service

oder Fragen per Mail an:

Mail2@volkerschroer.de

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

Liebe(r) Leser(in),*

Datenschutz → praktisch einfach und hilfreich!

Wenn die Grundlagen einmal gelegt, sind die Abläufe meist schlank (verschlankt), der Aufwand gering und mehr Zeit wie Sicherheit gewonnen.

Höchstrichterliche Entscheidung fallen erst nach und nach. An einer gemeinsamen Sprache von Juristen (Datenschutz), Informatikern (IT-Sicherheit) und Praktikern wird noch kräftig gefeilt. Von Datenschutzberater, Datenschutzberatung, Datenschutzmanagement bis zertifizierter, externer Datenschutzbeauftragter für Selbständige, Gewerbetreibende und KMU.

Sprechen wir!

Vielen Dank für Ihr Interesse

PS: Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist, oder kontaktieren Sie mich gerne.

HINWEISE:

Das Inhaltsverzeichnis finden Sie auf Seite 2:

- ✔ Die Einzelthemen können mit einem Mausklick direkt ansteuern
- ✔ Mit der Suche <Strg + F> können Sie auch Ihr Thema direkt ansteuern
- ✔ Quellenangaben sind hier statt als Fußnote als Endnote (am Ende des Dokuments) aufgeführt. Es macht diese Jahresarchiv übersichtlicher.
- ✔ Die Themen sind aus den Monatsinformationen angefügt. Den jeweiligen Monat können Sie am Textanfang durch folgenden Hinweis erkennen: „##/2021“.

06/2021 *Das Bundesamt: „Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)“ hat seine Homepage vollständig überarbeitet, wodurch bisherige Verknüpfungen zu einer Fehlermeldung führen. Auf meiner Seite im Netz, wie in den „Zusammenfassungen | Muster | Vorlagen | Mail - Anlagen (Stand)“ habe ich die Verknüpfungen korrigiert und ab jetzt auch in den Informationsbriefen. Nur im Archiv war mir eine Anpassung der Informationsbriefe nicht mehr möglich.* [1]

06/2021 Das Bundesdatenschutzgesetz feiert 45 – jähriges Jubiläum in der dritten Fassung [2]

(1) Standard – Datenschutz - Modell Vers. 2.0b

Mit dem SDM verfolgt die Datenschutzkonferenz (DSK) der Aufsichtsbehörden des Bundes und der Länder eine „gemeinsame Sprache der Juristen und Informatiker“ für die Verantwortlichen und Datenschutzpraktiker zu finden. Letzte Fassung vom 17.04.2020

Zum aktuellen SDM der Aufsicht (72 Seiten; Link in Bild & Text)	**Zur Zusammenfassung des SDM (10 Seiten; Link in Bild & Text)**

Letzte Ergänzung: 11/2021

03/2021 Am 25.03.2021 wurde der Baustein „41. Planen und Spezifizieren“ des Maßnahmenkatalogs bei hohem bis sehr hohem Risiko der Daten veröffentlicht, mit Details zu den 3 Faktoren der Entscheidung in der Planungsphase: 1. Kontrollieren, 2. Prüfen und 3. Beurteilen.

11/2021 Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“ (Version 1.0 vom 01.11.2021)[3] Das Wesentliche (1 S.) und eine Musterrichtlinie zum Berechtigungskonzept (2.S.; hier klicken)

Inhalte 2021

(Einfach gesuchtes Thema <Strg+F> und oder nach Wahl anklicken)

(2) Zum Datenschutz

(a) Corona: SARS-CoV-X = AHA+L-4G(+A)(+I)?

01/2021 Die Formel gegen den Corona – Virus?! Der Arbeitgeber[4] hat die Pflicht dafür zu sorgen, dass der Mitarbeiter arbeiten kann, ohne sich gesundheitlichen Gefahren auszusetzen. Das bedeutet die strenge Einhaltung der Hygienevorschriften „AHA – Regeln“ (Abstand, Hygiene, Atemschutz[5]) „+L“ (regelmäßiges Lüften) „-4G“ (Vermeidung von geschlossenen Räumen, Gruppen und Gedränge, Gespräche in lebhafter Atmosphäre) „(+A)“ für die Corona – App, die aber nicht vorgeschrieben, geschweige den kontrolliert werden darf. „(+I)“ Es besteht keine Impflicht, diese kann auch nicht vorgeschrieben, oder über Nachweise kontrolliert werden und es sollte auch kein Druck auf die Mitarbeiter dazu ausgeübt werden[6]. Die Fürsorge kann auch durch Klauseln im Arbeitsvertrag nicht aufgehoben oder eingeschränkt werden. Weiter Hinweise zur Fürsorge- und Meldepflicht per Link in der Fußnote[7]. (+A) und (+I) fällt wegen sensibler Gesundheitsdaten unter besondere Kategorien[8] des Datenschutzes. Eine Ausnahme[4] gilt lediglich für RKI, Ärzte, Krankenhäuser im Rahmen des Infektionsschutzgesetzes zum Schutz der Gesundheit der Person. UND: „Merkel verteidigt Datenschutz der Corona – App“ bei golem.de – Recht gut finde ich[5].

(b) Prognosen und Offenbarungen 2021

01/2021 In einem Artikel von Security-Insider, warnt Mareike Vogt als Fachexpertin Datenschutz der TÜV SÜD Sec-IT, vor Nachlässigkeit beim Schutz von Kundendaten und erklärt, wie man 2021 die größten Stolpersteine vermeidet.[9] Stichworte sind: „EuGH – Schrems II“ Datenschutz außerhalb der EU, vor allem die großen US – Anbieter, „BREXIT“ da Großbritannien jetzt auch zum EU – Drittland zählt und „Home-Office“ mit sicheren IT-Zugriffen. Als häufige Datenschutzsünden wird angeführt auf Platz 3: „Fehlende Einbindung des Datenschutzbeauftragten, Platz 2: „Mangelnder Fokus auf IT-Sicherheit“ und auf Platz 1: „Fehlende Zuteilung von Ressourcen“.

Hinzu kommen noch gesteigerte Aktivitäten der Cyber – Kriminalität in Form von Hacks, Manipulation von Algorithmen, KI – Angriffe, Deepfake Angriffe über Video, Audio und Bild, Social – Media Attacken, Identitätsdiebstahl[5]. Plus dem damit verbundenen Dokumentations- und Meldeaufwand.

(c) Messenger: Privat ist Ihre Sache (fast), aber ...

01/2021 Der Aufreger ist die AGB – (Zwangs-) Änderung von WhatsApp. Für den Privatbereich gibt es ja die „Haushaltsausnahme“, die allerdings da endet, wo Sie meine Daten (Kontaktdaten, Text, Bild, Ton, Video u.s.w.) ohne meine Erlaubnis verwenden. Geschäftlich sieht das völlig anders aus!

i) Drei wesentlichen Punkte

Zunächst ist der Sitz des Unternehmens in den USA und nach dem EuGH – Urteil (Schrems II) ein EU – Drittland ohne Angemessenheitsbeschluss (EU zertifiziert), ohne akzeptierte Unternehmens-zertifizierungen & Standardvertragsklauseln und nicht im Einklang mit lokalen gesetzlichen Regelungen (z. B. USA: FISA - Foreign Intelligence Surveillance Act).

Nach Unternehmensangaben sind die Nutzer in Europa wegen der DS-GVO nicht betroffen, allerdings räumt Facebook sich das Recht ein, die Daten zu nutzen, um „*unsere Dienste zu betreiben, bereitzustellen, zu verbessern, zu verstehen, anzupassen, zu unterstützen und zu vermarkten*“. („Wer einmal lügt, dem glaubt man nicht“).

Dazu kommt dann die (nicht ganz zwingende) Freigab des Telefon – Adressbuches. Da bestehen doch Zweifel, ob jeder in ihrem Adressbuch die Freigabe zur Weitergabe an Facebook/WhatsApp zugestimmt hat. [10]

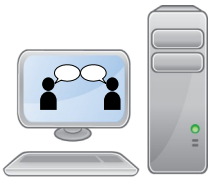
ii) Keine Geheimnisse?

„Ich habe doch nichts zu verbergen und reich bin ich auch nicht!“? Mit den „Meta-Daten“ auch aus anderen Quellen können Persönlichkeits- und Beziehungsprofile erstellt werden. Damit bieten sich Beeinflussungsmöglichkeiten und mindestens die Eignung als Testopfer für Angriffe (Hacks).

iii) Alternativen?

Wesentlicher Punkt bei der Auswahl eines geeigneten Messenger im geschäftlichen Umfeld sollte die Einhaltung der DS-GVO sein, da Sie als Verantwortlicher der Daten diese in jedem Fall nachweisbar erfüllen müssen. Ohne hier Werbung für einzelne Messenger machen zu wollen und ohne Anspruch auf Vollständigkeit, ein paar Alternativen aus Europa: THREEMA (Threema GmbH, Pfäffikon/CH), WIRE (Wire Swiss GmbH, Zug/CH), GRAPE (UberGrape GmbH, Wien/AT), GINLO (ginlo.net GmbH, München/DE)[11].

iv) Wo wir gerade … noch zu Videokonferenz Tools



Gibt es das EINE, WAHRE Video – Konferenz – Tool? Ich vermute: „Nein“! Jetzt schaue ich hier nicht auf die Funktionalitäten, die sehr unterschiedlich in den Anforderungen sein können und die jeder / jedes Unternehmer/en selbst festlegen sollte, sondern mehr auf eine Datenschutzkonformität. Aber auch dazu schätzte ich derzeit: „Jein!“. Wie immer stellen die Aufsichtsbehörden umfangreiches Informationsmaterial zur Verfügung (BSI ca. 170 Seiten, BfDI ca. 25 Seiten), erkennen aber auch an, dass derzeit keine Lösung volle Funktionalität und Datenschutz bietet. Für einen angemessen Datenschutz in der aktuellen Situation (Home-Office) werden zur Auswahl drei Schwerpunkte vorgeschlagen: 1.) Transparenz in Bezug auf Nutzung und Datenverarbeitung 2.) Sicherheit in Bezug auf Nutzer – Authentifizierung und Vollverschlüsselung 3.) Eingriffsmöglichkeiten der Nutzer auf Inhalte, Metadaten und Bestandsdaten (ändern, löschen). Mehr von der Bundesaufsicht über den Link in der Fußnote[12]. Das Europäisches Zentrum für digitale Rechte in Wien (noyb, Nicht-Regierungs-Organisation) hat übersichtlich die (Nicht-) Erfüllung der DS-GVO zu den Hauptanbietern zusammengestellt (Link Fußnote[13]). Eine Sache noch, wenn Sie zu einer Videokonferenz einladen, klären Sie mit der Einladung transparent und verständlich über den (nicht) gegebenen Datenschutz auf. Einige Entwürfe finden Sie auf meiner Netzseite.

(d) Kleines, schlankes Verfahrensverzeichnis

02/2021 Schön ist es doch, wenn nicht alle „Größen“ in ein Format gepresst werden müssen, sondern die vorgeschriebenen Anforderung frei formatiert werden können. So kann der Aufwand für die Dokumentation (auch Bürokratie genannt) auf den praktischen Bedarf beschränkt bleiben.

i) Ziel des Verfahrensverzeichnisses

.. nach dem Erwägungsgrund (82) der DS-GVO[14]

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

*ii) Vorschriften (1*Form, 6*Inhalt, 1*Hinweis)*

Aus der DS-GVO Art.30[15] und dem BDSG §70[16] ergeben sich folgende Mindestanforderungen:

(Form^2) Dokumentation in schriftlichem oder auch in elektronischem, unterzeichnetem Format

- (1^2) Name und Kontaktdaten von Verantwortlichen und ggf. Datenschutzbeauftragen
- (2^2) Beschreibung von Zweck der Verarbeitung und der Kategorien der Personen und Daten
- (3^2) Wer erhält Daten (interne & externe Empfänger in Europa, Drittland, internationale Organisation) und wie wird die Einhaltung der Datenschutzvorschriften gewährleistet.
- (4^2) Wenn möglich vorgesehen Löschfristen und - wenn möglich - eine Beschreibung der technisch - organisatorische Schutzmaßnahmen
- (5^3) Rechtsgrundlage der Verarbeitung
- (6^3) Alternativ zu Löschfristen die Überprüfungstermine zur Notwendigkeit

(Hinweis^2) Die gleichen Angaben sind für Auftragsverarbeiter (Dienstleister) zu dokumentieren

iii) Beispielmuster

Finden Sie auf meiner Seite im Netz ein Zusammenfassung (1-Seite) und einen Vorschlag für ein kleines, schlankes Verfahrensverzeichnis (und etwas mehr) unter:
https://volkerschroer.de/DSGVO/2021.02.28.Kleines.Verfahrensverzeichnis.Minimum.pdf

(e) Die Sache mit der Rückverfolgbarkeit ...

02/2021 … nach §4a Corona Schutzverordnung vom 30.11.2020[17] i.V.m. den Hinweisen des LDI (Landesbeauftragte für Datenschutz und Informationsfreiheit NRW)[18]. Die Friseure dürfen ja ab 01. März wieder unter Corona – Auflagen öffnen. Andeutungsweise war auch, natürlich unter bestimmten Bedingungen, von der Öffnung des Einzelhandels und weiterer („körpernaher“) Dienstleistung zu hören. Das setzt die Kontaktrückverfolgbarkeit wieder in Kraft und erinnert an die unterschiedlichsten Datenerhebungsformen. Die Formularvorlage des LDI NRW, welche aus Niedersachsen mit „copy&paste“ übernommen wurde, ist mit 2 Seiten nicht gerade übersichtlich, zumal die Aufbewahrungsfrist in NRW 4 statt 3 Wochen ist und die zuständige Aufsichtsbehörde nicht Niedersachsen sondern hier in NRW ist.

(f) Rückverfolgung – 1 Seite – Papier &/o Digital

02/2021 Auf Basis der CoronaSchVO in NRW und des Vorschlags der Datenschutzaufsicht NRW habe ich ein 1-seitiges Formular zum ausfüllen im PDF – Format entworfen zur handschriftlichen Nutzung oder digitalem Ausfüllen mit der Möglichkeit nur zu drucken und/oder nur zu speichern. Die räumliche Verteilung in Verbindung mit einem Raumplan ist integriert, z. B. für Restaurants, Studios, Vereinssitzungen u. ä. Sie finden das Formular zur freien Verwendung auf meiner Netzseite unter: https://volkerschroer.de/DSGVO/2021.02.28.IfSG.Nachverfolgungsmeldung.pdf

(g) DS-GVO.clever – LfDI-Tool für Vereine

02/2021 Ich mache mal Werbung für die Aufsicht (LfDI) Baden – Württemberg. Dort hat man für (kleinere) Vereine ein Tool (DS-GVO.clever) ins Netz gestellt und bietet dazu auch ein Webinar an[19]. Mit den Angaben auf der rechten Seite wird Text für die Datenschutzerklärung / Impressum zum kopieren in der linken Spalte angeboten. Beim Ausfüllen werden wichtige Hinweise gegeben.

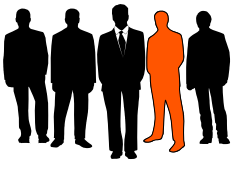
(h) BREXIT Übergangsverlängerung bis 30.06.2021

02/2021 Mit dem Austritt Großbritanniens zum 31.12.2020 aus der EU, gilt GB als Drittland und es muss der Nachweis über die DS-GVO Konformität erbracht werden (Pauschal z. B. über einen Angemessenheitsbeschluss der EU). Am 19. Februar 2021 leitete die Kommission das Verfahren für die Annahme von zwei Angemessenheitsentscheidungen für die Übermittlung personenbezogener Daten an das Vereinigte Königreich als EU-Drittland gemäß der Allgemeinen Datenschutzverordnung (DSGVO) ein. Bis zur Annahme ist die Übergangsphase bis maximal 30.06.2021 gemäß Abkommen verlängert.[20]

(i) Pseudo- oder Anonym

03/2021 Allgemeine Definition von Anonymität[21]: „*Nichtbekanntsein, Nichtgenanntsein; Namenlosigkeit*“ und von Pseudonymität[22]: „*Pseudonymität ist ein Zustand, bei dem Daten nicht unmittelbar der Person (betroffenen Person) zugeordnet werden können.*“

i) Im Datenschutzgesetz



DS-GVO Erwägungsgrund[23]: „*(26) Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, … sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. ... personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.*“

DS-GVO Art.4 Nr.5[24]: „*"Pseudonymisierung" die Verarbeitung … in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.*“

ii) Von der Aufsicht

In einem Positionspapier hält der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit fest[25]: „*Eine absolute Anonymisierung derart, dass die Wiederherstellung des Personenbezugs für niemanden möglich ist, dürfte häufig nicht möglich sein und ist im Regelfall datenschutzrechtlich auch nicht gefordert. Ausreichend ist in der Regel, dass der Personenbezug derart aufgehoben wird, dass eine Re-Identifizierung praktisch nicht durchführbar ist, weil der Personenbezug nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden kann.*“

iii) Was bringt’s (Fazit):

1. Der Datenschutz gilt nicht für anonyme Daten, d. h. keine direkte (Name, Adresse, Telefon usw.) oder indirekte (Vergleich über Gruppen, Merkmale u.ä.) Identifizierung der natürlichen Person.
2. Die Pseudonymisierung (Schutz und Separierung von Identitätsdaten) ist ein geeignetes technisch – organisatorisches Mittel zur Erhöhung des Schutzniveaus zur Senkung des Risikos, z. B. für die besonderen Kategorien von Daten nach der DS-GVO[26].

(j) Wie jetzt(?): „Finger weg von der Cloud“, was’n passiert?

03/2021 … da hätte die richtige Pseudonymisierung ein hilfreicher Baustein sein können. Was war passiert? Wie Cloudcomputing – Insider berichtet „*Deutsche Psychotherapeuten warnen vor der Cloud*“[27], sind in Frankreich 500.000 Datensätze dem französischen Ableger des auf Software im Gesundheitswesen spezialisierten Unternehmens Dedalus geklaut und veröffentlicht worden. Neben Namen und umfangreichen Kontaktdaten sind auch teils Angaben zum Gesundheitszustand, Medikation, Schwangerschaften, Krankheiten und Diagnosen gestohlen und veröffentlicht.

(k) Wie umgehen mit Corona – Firmentestergebnissen?

04/2021 Aus der Corona – Formel: „*SARS-CoV-X = AHA+L-4G(+A)(+I)*“ im Informationsbrief vom Januar[28] ist bekannt, dass die Corona – Test - Ergebnisse zu den besonders schützenswerten Gesundheitsdaten nach Art. 9 DS-GVO gehören. Nach Absatz (1) ist die Verarbeitung grundsätzlich untersagt. Ausnahme (z. B.) nach Abs. (2) lit. h) gilt für Zwecke der Gesundheitsvorsorge, aber nur bei Verarbeitung durch Fachpersonal gemäß Abs. (3), also für RKI, Ärzte, Krankenhäuser im Rahmen des Infektionsschutzgesetzes. Ein weitere Ausnahme nach Abs.2 lit. a) ist eine ausdrückliche und freiwillige Einwilligung, was in einem Beschäftigungsverhältnis problematisch ist, oder nach Abs.2 lit. c) zum Schutz lebenswichtiger Interessen des Betroffenen oder einer anderen natürlichen Person. Dazu besteht eine Meldepflicht nach dem Infektionsschutzgesetzes §8 Abs. (4)[29] „*für Personen, die die Untersuchung zum Nachweis von Krankheitserregern außerhalb des Geltungsbereichs dieses Gesetzes durchführen lassen.*“ In einer Pressemitteilung[30] fordert die Datenschutzkonferenz der Länder den Gesetzgeber zu einer eindeutigen Regelung für die pandemische Lage auf. Aus der Liste[31] der Datenschutzkonferenz zu den Verarbeitungstätigkeiten (DSK – MUSS – Liste, Nr. 15 - 17) ist bei Gesundheitsdaten eine Datenschutz – Folgenabschätzung vorzunehmen und zu dokumentieren. Unter Berücksichtigung der Ausführungen zur Testpflicht vom 19.04.2021 auf „anwalt.de“[32] ist mein praktische Vorschlag:

- ✔ Freiwilliges, anonymes Testangebot vor (bzw. bei) Zutrittskontrolle. Ein Nachweise des Angebots ist sicher jederzeit über Quittungen / Rechnungen möglich.
- ✔ Eine Verhaltensregel, dass alle Testergebnisse in einem verschlossen Umschlag mit Namensaufschrift abzugeben sind und diese für kurze Zeit* aufbewahrt werden. Verpflichtend ist bei einem positiven Test umgehend einen Arzt für einen bestätigenden PCR – Test aufzusuchen, gegebenenfalls zwischenzeitliche Kontakte zu informieren und eine allgemeine Krankmeldung / Arztbesuch vorzunehmen.

*) *Die Aufbewahrungszeit, da nicht gesetzlich geregelt, wird zur Zeit unterschiedlich ausgelegt. Nach dem IfSG sind Nachverfolgungsnachweise für das Gesundheitsamt 4 Wochen (NRW) vorzuhalten.*

- ✔ Die verschlossenen Testergebnisse sind sicher aufzubewahren und der Zugang sollte auf einen sehr eng begrenzen Personenkreis beschränkt sein, der auch nach Ablauf der Aufbewahrungszeit die anonyme Vernichtung vornimmt. Auf eine Datenverarbeitung sollte verzichtet werden.

[***Nur eine Idee …*** *Um die Infektionsnachverfolgung zu unterstützen könnte die Corona – Warn – App mit einem QR – Code – Event (Ort)*[33] *genutzt werden oder das Rückverfolgungsformular (ohne den Satz unter Punkt 2. „... nicht bedienen …)*[34].]

[***Vorsicht …*** *grundsätzlich besteht keine Mitarbeitertestpflicht, auf der anderen Seite besteht eine Fürsorgepflicht des Arbeitgebers für die Beschäftigten und einzelne Bundesländer haben z. B. für „körpernahe Tätigkeiten“ wie Berlin eine bestimmt. Es bedeutet zwar nicht, dass ein Arbeitnehmer gezwungen werden kann, einen Test durchzuführen. Weigert er sich, kann er aber die geschuldete Arbeitsleistung nicht erbringen und erhält dann auch keine Vergütung“, so der Fachanwalt für Arbeitsrecht, Rechtsanwalt Thomas Niklas, Kanzlei Küttner in einem Artikel auf Welt-Online* [35]]

(l) Drittlandstransfer prüfen, es wird Zeit?!

04/2021 Beispielhaft ein Artikel im Handelsblatt vom 13.04.2021: „*Deutsche Firmen in der Datenschutzfalle – Behörden intensivieren Ermittlungen wegen US – Cloud – Nutzung*“[36] Hintergrund war das Urteil des EuGH „*Schrems ii*“, mit dem das Abkommen „EU - US – Privacy - Shield“ kassiert, auch Standard-vertragsklausel auf ihre Durchsetzbarkeit im Einzelfall zu prüfen sind und laut Gericht diese z. B. bei Unternehmen die der US – Jurisdiktion unterliegen. Dabei ist es egal, wo auf der Welt die Daten gespeichert sind. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat hierzu ein Prüfschema veröffentlicht[37]. Ich habe mir erlaubt das Prüfschema in 7 Fragen zum Ankreuzen auf einer Seite zusammenzufassen. Prüfen und dokumentieren in einem, auf einer Seite zum Nachweise (Abbild mit Link).


Für den eiligen Leser kurz zusammengetragen (1/1)

Checkliste – Drittlandstransfer

Kurz mal durchgeprüft

Nach dem Artikel vom 13.04.2021 im Handelsblatt" nimmt die Aufsicht eine verschärfte Prüfung des Drittlandstransfers nach dem EuGH – Urteil „Schrems II" vor. Vor Prüfung des Drittlandstransfers sollten zunächst natürlich die anderen Voraussetzung nach der DS-GVO für die Datenverarbeitung innerhalb der EU gegeben sein – versteht sich. Dann ist folgende Prüfung vorzunehmen

(1) Wenden personenbezogene Daten an Drittländer außerhalb der EU „offen gelegt"?

☐ JA weiter zu 2 ☐ NEIN – Ende siehe Nr. (7)

(2) Sind die Daten so verschlüsselt, dass im Drittland kein Zugriff möglich ist?

☐ NEIN weiter zu 3 ☐ JA – Ende siehe Nr. (7)

(3) Liegt ein Angemessenheitsbeschluss" der EU für das Drittland vor?

☐ NEIN weiter zu 4 ☐ JA – Ende siehe Nr. (7)

(4) Kann mit der Auswahl von bzw. der Schutzmaßnahmen nach Kapitel V der DS – GVO ein gleichwertiges Schutzniveau gewährleistet werden?

Im besonderen Artikel 46 „Datenübermittlung vorbehaltlich geeigneter Garantien" und Artikel 47 „Verbindliche interne Datenschutzvorschriften", sowie Artikel 45 DS-GVO for Gerichtsbeschluss im Drittland. (z. B. Standard – Datenschutzklauseln. Interne Datenschutzvorschriften durchsetzbare Rechte, und Rechtsbehelfe mit wirksamen Mechanismen im Drittland)

☐ NEIN weiter zu 5 ☐ JA – Ende siehe Nr. (7)

(5) Können zusätzliche Schutzmaßnahmen definiert und ergriffen werden, um ein gleichwertiges Schutzniveau der DS – GVO zu erlangen?

Damit ein gleichwertiges Schutzniveau erreicht wird müssen nach dem EuGH – Urteil zusätzliche Maßnahmen in technischer, organisatorischer oder rechtlicher Hinsicht ergriffen werden, um die Gleichwertigkeit zu erreichen. Bei vertraglichen Anpassungen in Abweichung zu den Standard – Datenschutzklauseln sind diese als „schon-Klauseln" VORAB durch die Aufsichtsbehörde zu genehmigen.

☐ NEIN – Einsatz Alternative ☐ JA weiter zu 6

(6) Sind die zusätzlichen Schutzmaßnahmen umgesetzt und praktisch wirksam?

☐ NEIN – Einsatz Alternative ☐ JA weiter zu 7

(7) Sind Maßnahmen und die Prüfung dokumentiert?

In jedem Fall (Nachweispflichten) ist die Prüfung und das Ergebnis des Datentransfers zu dokumentieren und im Verfahrensverzeichnis nachprüfbar für die Aufsichtsbehörde zu dokumentieren, neben einer transparenten Aufklärung (Effekt) der „Betroffenen" und deren Einwilligung

☐ NEIN – es wird Zeit ☐ JA – PERFEKT

HINWEISE:

Wird der Datentransfer in ein Drittland trotz Mängel im Schutzniveau (unzulässiger Weise) fortgeführt, besteht eine MELDEPFLICHT gegenüber der Aufsichtsbehörde!

Ja, es gibt eine Ausnahme nach DS – GVO Art. 49 „AUSNAHME FÜR BESTIMMTE FÄLLE" (a) Risikoaufklärung mit ausdrücklicher Zustimmung, (b) Vertragserfüllung oder (c) bei Rechtsansprüchen u. a. Nach Art.49 (1) 2. Abs. „... darf eine Übermittlung an ein Drittland ... nur dann ... wenn ... nicht wiederholt erfolgt, nur eine begrenzte Zahl ... betrifft ..." ... oben Ausnahmetatbestände"

Abb.: Checkliste (PDF) prüfen und dokumentieren auf 1. Seite einfach anklicken (LINK)

Hinweise:

- ✖ Wird der Datentransfer in ein Drittland trotz Mängel im Schutzniveau (unzulässiger Weise) fortgeführt, besteht eine MELDEPFLICHT gegenüber der Aufsichtsbehörde!
- ✖ Ja, es gibt eine Ausnahme nach DS – GVO Art. 49[38] „AUSNAHME FÜR BESTIMMTE FÄLLE“, allerdings mit starkem Ausnahmecharakter für ganz bestimmte Fälle und wenn „*… nicht wiederholt erfolgt, nur eine begrenzte Zahl …*“

(m) Womit wir bei MS 365 wären

04/2021 Da noch keine Einigkeit erzielt, „brodelt“ es weiter in den Aufsichtsbehörden. Das Ergebnis der Prüfung durch die Datenschutzkonferenz der Ländern zu MS 365 (Office-Suite) ist: „nicht daten-schutzkonform einsetzbar“. Ein Positionspapier[39] wurde mit 9 zu 8 Stimmen knapp angenommen. Wegen „rechtlich, fragwürdiger Ausführungen“ konnte bisher keine Entscheidung zur Veröffentlichung getroffen werden, aber das Ergebnis bleibt.

- FRAGE: Kann Microsoft 365 jetzt nun genutzt werden oder nicht?
  ANTWORT: „Na ja, wenn …!“
- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat bisher noch keinen Baustein im IT - Grundschutz veröffentlicht, aber eine Empfehlung für die Konfiguration von Microsoft – Office bzw. 365 veröffentlicht (Link in den Fußnoten)[40]. Macht die Anwendungen sicherer, aber noch nicht perfekt für den Schutz von (nicht nur) personenbezogenen Daten.
- Zur Absicherung sollte eine Datenschutz – Folgenabschätzung geprüft werden und diese wird hier sicherlich mit Dokumentation erforderlich sein. Schritt 1: Erfassung und Beschreibung der Datenverarbeitungsvorgänge mit Zweck, rechtliche Grundlage, und Notwendigkeit. Schritt 2: Begründung der Verhältnismäßigkeit (Beispiel). a.) Es wird ein legitimer Zweck verfolgt b.) Ist zur Zweckerreichung geeignet. c.) Es steht kein gleichwertiges, wirksames Mittel zur Verfügung d.) Das Interesse des Unternehmens überwiegt die Interessen der Betroffenen (DSGVO Art.6 Abs.1 lit.(f) i.V. m. ErwG.47[41]). Unternehmensinteressen: Übergreifende Zusammenarbeit mit Dritten, Diagnosedaten zur Fehlbehebung, Synchronisation von Cloud und Endgeräten. Schritt 3: Das Risiko bewerten und beheben. Microsoft bietet dazu auch eine umfangreiche Unterstützung bei der Bewertung an[42]. Unter Berücksichtigung der möglichen Schadenshöhe und der Eintrittswahrscheinlichkeit (siehe Punkt 1, Kurzfassung SDM Seit 6,7) sollte eine

geringes, bis normales Risiko nicht überschritten werden. Zur Risikoreduzierung können zusätzliche organisatorische Maßnahmen wie Schulungen, Rollen- und Berechtigungskonzepte ergänzt werden.

➤ FAZIT: „… ja weitestgehend, wenn“ in einer dokumentierten Risikoeinschätzung kein hohes Risiko für die Betroffenen, ein berechtigtes Interesse für den Verantwortlichen / die Organisation besteht und eine vergleichbare Alternative nicht zur Verfügung steht. Das senkt auf jeden Fall deutlich das Risiko vor möglich Regressansprüchen und Bußgeldern. *(Natürlich ist es besser, sich nach möglichen Alternativen umzuschauen, um auf der ganz sicheren Seite zu sein.)*

(n) DSGVO : Klagen über zu viel Bürokratie?

05/2021 In regelmäßigen Abständen ist über Klagen von zu viel Bürokratie zum Datenschutz zu lesen. Beispielhaft zwei Artikel als Link in den Fußnoten [43]. Wie bei allen Problemstellungen hängt der UMFANG von der Größe der Organisation in Bezug auf die Quantität, nicht der Qualität ab.

i) JA,

… zu Beginn, wenn die Grundlagen dafür geschaffen werden müssen, wobei viele der Anforderungen bereits oft geschaffen sind. Bei der Analyse bezieht sich ein nicht unerheblicher Teil auf die Optimierung der Abläufe, was weniger mit der Bürokratie zum Datenschutz zu tun hat. Drei Fragen, die alles Wesentliche zu einer Verarbeitungstätigkeit abdecken:

1) Ist der Kunde vollumfänglich und leicht verständlich über Art, Zweck, Dauer und Verarbeitung seiner erhobenen Daten informiert und hat genau dazu sein Einverständnis gegeben?
2) Kann einer Aufforderung zum Nachweis, Auskunft, Berichtigung, Löschung, Vergessen, Übertragung sowie Widerspruch jederzeit und fristgerecht nachgekommen werden?
3) Kann Vertraulichkeit je nach Sensibilität, Integrität und Verfügbarkeit der erhobenen Daten jederzeit gewährleistet werden?

Wenn die drei Fragen mit „JA“ beantwortet werden können, ist zum sicheren Nachweis eine Dokumentation *im eigenen Interesse* zu erstellen, was in der DS-GVO als Verfahrensverzeichnis verankert ist. Die Dokumentationsanforderungen finden sie hier als Link zu „PDF“ mit Erläuterungen und als Mustervorlage als „DOCX“ oder „ODT“. Wie einfach es geht, zeigt auch das Muster für eine Arztpraxis des Bay. Landesamtes für Datenschutz mit nur einer Seite => LINK.

ii) NEIN,

… Datenschutz kann so einfach sein, wenn die Grundlagen dazu einmal gelegt sind, ist der kontinuierliche Prozess recht schlank zu halten. Miet- & Kauftools sind ein Frage von Quantität der Prozesse und der Organisation, nicht von Qualität. Neben einer regelmäßigen Information (z. B. eines monatlichen Informationsbriefes) und einer jährlichen „Wiedervorlage“ sind Anpassungen nur bei Änderungen oder neuen Verarbeitungen notwendig. Ein Berater sollte praktische und einfach unkomplizierte Hilfestellung leisten.

(o) Drittlandtransfer „zusätzliche Maßnahmen“

05/2021 Die Diskussion unter den Stichworten DS-GVO und „EuGH-Urteil, Schrems II, Exteritoriale EU Cloud“ geht in unverminderter Häufigkeit weiter. Neben der einseitigen Checkliste zum Drittlandtransfer im letzten Informationsbrief [44] hier noch die Empfehlungen des europäischen Datenschutzausschuss. Was sind zusätzliche Maßnahmen zur Erreichung eines gleichwertigen Datenschutzniveaus? Mit dieser Frage wollte uns der europäische Datenschutzausschuss (EDSA) nicht „alleine lassen“ und hat die Frage von sich aus untersucht und (nur) Empfehlungen auf 46 Seiten (12/2020) [45] ausgesprochen. Einen Link zu meiner Zusammenfassung auf 2 Seiten befindet sich in der Fußnote: [46]).

i) Hinweise

Die Prüfung eines DS-GVO konformen Datenschutzes gilt für die Verarbeitung in einem Drittland, als auch für die Speicherung (insbesondere Cloud) und die Durchleitung! Sobald auf die Übermittlungsinstrumente (Art.46ff DS-GVO) abgestellt wird, ist IMMER EINE WIRKSAMKEIT im Hinblick auf die Gesamtumstände zu prüfen und zu beurteilen. Die zusätzlichen Maßnahmen

dürfen die Instrumente (ohne Genehmigung der Aufsicht) nur ergänzen, müssen effektiv sein und die festgestellten Rechtsschutzlücken schließen.
X Auftragsverarbeitung und Transfer mit Zugriff in einem unsicheren Drittland sind nicht möglich, auch innerhalb einer Unternehmensgruppe und/oder eines gemeinsamen Geschäftszwecks!

ii) Empfehlung technische Maßnahmen

Empfohlen wird eine *Verschlüsselung vor Transfer* (z. B. in eine Cloud) *oder Drittlanddurchleitung* mit Zugriff nur aus dem Geltungsbereich der DS-GVO. Eine *Psydonymisierung vor Transfer* bei der die einzelnen Personen weder direkt, noch in einer größeren Gruppe außerhalb des Geltungsbereich der DS-GVO identifiziert werden können. *Geschützte Empfänger* (Geheimhaltungspflicht auch gegenüber Behörden) können Daten bei exklusivem Zugriff (End-to-End) erhalten. Die Vergabe von geteilten Daten zur Auftragsverarbeitung, die eine Identifizierung durch den Empfänger oder der Landesbehörden unmöglich macht und nur im Bereich der DS-GVO zusammengeführt werden können (Mulit-Party-Processing)

iii) Vertragliche und organisatorische Maßnahmen

Die Empfehlung des EDSA gehen hier in die Richtung von *mehr Transparenz* (Protokolle, Zugangsprüfungen, Information über Auskunftsanfragen, *zusätzliche Unterstützungspflichten* (Information, auch der Betroffenen, sowie lokale rechtliche Unterstützung), Vorgaben zur Datenminimierung, Normen und Verfahren und verbunden mit Kündigungsklauseln.

iv) Einschätzung:

- Wie der Ausschus (EDSA) schreibt, bleibt es im Einzelfall dem Verantwortlich auf Basis aller, im möglichen, zugänglichen Informationen zu prüfen, welche Rechtslücken bestehen und ob mit den zusätzlichen Maßnahmen diese geschlossen werden.
- Sofern die „Rechtsschutzlücken“ nicht durch Gerichte, Behörden oder vertrauenswürdige Institutionen und die Effektivität der zusätzlichen Maßnahmen eindeutig festgestellt wurde, ist m. E. ein Rechtsgutachten (Legal Opinion) durch einen lokalen Jurist unumgänglich.

(p) Ärger mit & über die Cookie – Banner

06/2021 Der Name „Schrems“ ist durch das EuGH – Urteil schon gut bekannt. Er ist auch Gründer des NGO (Nichtregierungsorganisation) „NOYB – europäisches Zentrum für digitale Rechte“ was aus „none of your businiess“, oder „geht Dich nichts an“ abgeleitet ist. Wie die Tagesschau[47] berichtet, ist eine groß angelegte, juristische Beschwerdewelle gegen rechtswidrige Cookie - Zustimmungsabfragen im Web geplant. 560 Unternehmen in Europa und der USA haben bereits einen Beschwerdebrief erhalten. Nach „NOYB“ gibt die DS-GVO ein klare Auswahl von „JA oder NEIN“ vor. Mit Tricks über komplexe Mehrfachklicks (Einstellungen), würden die Nutzer dazu verleitet den „Akzeptieren“-Button anzuklicken. NOYB hat zur Analyse eine Software entwickelt, die nach Analyse automatisch einen Beschwerdebrief generiert. Sofern nicht innerhalb einer Monatsfrist eine Anpassung erfolgt, wird die Beschwerde bei der zuständigen Aufsicht eingereicht.

(q) Und Tracking – Ärger, aber das schlimme daran …

06/2021 Die Zeit-Online berichtet[48] über einen Aktivisten, der vor dem Hamburger Landgericht gegen Onlinewerbung von (exemplarisch) 2 Unternehmen und den Onlinewerbeverband IAB Tech Lab klagt, die unberechtigter Weise persönliche Daten aus dem Surfverhalten an eine Vielzahl von Werbedienstleistern weitergeben. Die Daten aus dem Surfverhalten werden an eine große Zahl externer Dienstleister weitergereicht, die sie wiederum an Auktionsbörsen weitergeben um gezielte Werbung zu schalten. Das schlimme daran ist, der Branchenverband IAB Tech Lab hat einen technischen Standard für die Segmentierung der Nutzer veröffentlicht[49]. Nur aus dem Surfverhalten werden Kategorien wie "Verschuldung", "Unfruchtbarkeit", "Drogenmissbrauch" oder "Kinder mit Behinderung" gebildet. „*Wir warten mal mit Spannung auf das Urteil*“.

(r) Bußgelder Mai / Juni

- € 1,0 Mio. | IKEA Frankreich | Umfassende Ausspionierung der Mitarbeiter (LINK)

- € 1,2 Mio. | MedHelp AB Schweden | Ungeschützte Webspeicherung von Gesprächen einer Gesundheitshotline. (LINK)
- € 1,5 Mio. *2 | EDP – Gruppe Spanien | Vertragsabschlüsse mit unautorisierten Vertretern und mit Verletzung der Informationspflicht (LINK1 | LINK2)

(s) Drittlandtransfer ! Stichprobenprüfung der Aufsicht !

06/2021 Wie auf der Seite der hamburgischen Aufsichtsbehörde zu lesen, findet eine koordinierte Prüfung des internationaler Datentransfers[50] im Rahmen einer Fragebogenaktion zur Durchsetzung der Anforderungen des EuGH – Urteil Schremms II in Form von Stichproben bei ausgewählten Unternehmen statt. Dort können die Fragebögen (hier verlinkt) *E-Mail-Versand (PDF)*, *Hosting von Internet-Seiten (PDF)*, *Webtracking (PDF)*, *Verwaltung von Bewerberdaten (PDF)* und *konzern-internen Austausch von Kundendaten und Daten der Beschäftigten (PDF)* eingesehen werden.

Mit dem Durchführungsbeschluss der EU 2021/914 vom 4. Juni 2021 hat die EU neue Standard-vertragsklauseln (SVK) / Standard Contractual Clauses (SCC)[51] verabschiedet. Mit Modularem Aufbau für verschiedene Konstellationen (zu Verantwortlichem Auftragsverarbeiter). Siehe auch:

- ✔ Checkliste Drittlandtransfer (1 Seite 04/2021 Update 06/2021)
- ✔ Zusätzl. Maßnahmen EDSA (2 Seiten 05/2021 Update 06/2021)

28.6. *LINKS: BfDI | EU – PDF EU > Angemessenheitsbeschluss für UK > Datentransfer ohne weitere Prüfung! (ex Einwanderungskontrolle)*

(t) Alle hassen den Datenschutz – zu Unrecht

06/2021 Ist beim Datenschutz alles Gold was glänzt? Leider nicht. Mit kaum einem Argument kann man eine Diskussion so schnell beenden wie mit dem Verweis auf das vermeintliche Hindernis des Datenschutzes. Doch in Wahrheit ist der Datenschutz oft nur die Entschuldigung für eingefahrene Strukturen und bräsige Verwaltungen. 5 Mythen beschreibt K. Kuhle (FDP Bundestagsfraktion) in einem Blog auf ntv [52] sehr anschaulich.

(u) Aufsicht setzt Behörden eine Frist für Facebook - Nutzung

07/2021 Wie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Prof. Ulrich Kleber mit Schreiben vom 16.06.2021 an alle Bundesministerien und Bundesbehörden mitteilte (Auszug)[53],

„Ein längeres Abwarten ist mir angesichts der fortdauernden Verletzung des Schutzes personenbezogener Daten der Nutzerinnen und Nutzer nicht möglich. Sofern Sie eine Fanpage betreiben, empfehle ich Ihnen daher nachdrücklich, diese bis Ende diesen Jahres abzuschalten. Ab Januar 2022 beabsichtige ich – im Interesse der betroffenen Bürgerinnen und Bürger – schrittweise von den mir nach Art. 58 DSGVO zur Verfügung stehenden Abhilfemaßnahmen Gebrauch zu machen.“ „Zur Nutzung von WhatsApp verweise ich auf mein Rundschreiben vom 14. April 2020 (Az.: 24-190/020#2296)“

Das gilt gleichlaufend für WhatsApp, da hier auf den Drittlandtransfer (Schrems II – Urteil des EuGH) verwiesen wird.

i) Art.58 eine Drohung?

JA! In Art 58 DS-GVO sind die Befugnisse der Aufsichtsbehörde geregelt. Von Zugriff, Zutritt und Besichtigung von allen Räumen und Vorgängen (Art. 58 Abs.1 DS-GVO) bis zu Abhilfemaßnahmen einschließlich Verbot (Art.58 Abs.2 DS-GVO).

ii) Geht noch mehr?

JA! In dem Rundbrief hat der BfDI noch ***nicht*** auf die Art. 83 & 84 zu den allgemeinen Bedingungen für die Verhängung von Geldbußen (Art.83) und Sanktionen (Art.84 DS-GVO) hingewiesen.

iii) Die Gründe

Eine Fanpage wird immer gemeinsam mit Facebook betrieben, was zu einer „gemeinsame Verantwortung“ verpflichtet. Dies erfordert nach Art. 26 DS-GVO eine Vereinbarung mit Facebook dazu. Facebook stellt zwar seit 2019 eine Vereinbarung „Addendum“ zur Verfügung, allerdings wird dort für alle Informationspflichten an Facebook verwiesen. Damit können alle Fanpage – Betreiber ihren Pflichten nach Art.5 DS-GVO, den Grundsätzen für die Verarbeitung von personenbezogen Daten, nicht nachkommen bzw. sind abhängig von der „Offenheit, Schnelligkeit, Großzügigkeit und

Auskunftsfreudigkeit“ von Facebook (?). Alle bisherigen Konstruktionen auch von Länderaufsichtsbehörden könnten damit bald mehr oder weniger hinfällig *(„für die Tonne“) sein*. Nur ein „paar“ Anforderungen aus Art.5: Transparenz, Datenminimierung, Löschung, Auskunft, Zugriffsberechtigungen bzw. Kontaktdaten (Need-To-Know-Prinzip), Verwendung Metadaten u. a.

iv) Was kann uns da schon passieren?

„Der BfDI ist doch für den Bund / Behörden zuständig!“ JA UND für die Überwachung und Durchsetzung des Datenschutzes in Deutschland UND damit zentrale Koordinierungsstelle für die Landesbehörden UND innerhalb der europäischen Aufsicht![54]. Abgeleitet von der Aussage: „Wo kein Kläger, da kein Richter (bzw. Beklagter)“ könnte man sich in einer gewissen Sicherheit wiegen, wenn nicht als Kläger in Betracht kämen:

> verärgerte Kunden	> unzufriedene Mitarbeiter	> verärgerte Lieferanten
> Datenschutzaktivisten	> Aufsichtsbehörden	> Abmahn - Kanzleien

Es ist dann nur noch eine Frage der Zeit. Eine Empfehlung („wie auch immer“) zu Facebook / WhatsApp kann ich als Datenschutzbeauftragter also nicht aussprechen. Vielleicht informativ hilfreich, könnte ein Blick auf meine jetzt (bald?) hinfällige Vorlage „Datenschutzerklärung Facebook“ (Basis vom LfDI-RP) aus 06/2020 bis es zu einem endgültigen Urteil des EuGH kommt.

(v) Was sind: „gemeinsam Verantwortliche“

07/2021 Im Art.26 Abs.1 der DS-GVO lautet es:

„Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt.“

und in der Pressemitteilung des EuGH Nr. 81/18 vom 05.06.2018[55] zu Facebook:

„Der Betreiber einer Facebook - Fanpage ist gemeinsam mit Facebook für die Verarbeitung der personenbezogenen Daten der Besucher seiner Seite verantwortlich. … Ein solcher Betreiber ist ... an der Entscheidung über die Zwecke und Mittel … seiner Fanpage beteiligt. Nach Ansicht des Gerichtshofs kann der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, diesen nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien.“

Hinweise:

Viele „Dienstleiter“ (wie auch Auftragsverarbeiter) bieten auf Ihren Seiten bereits eine Vereinbarung, teilweise sogar „automatisch“ an. Eine Vorlage / Muster für die vertragliche Grundlage und die Information der Betroffenen habe ich hier (LINK) zur ersten Information erstellt.

(w) E – Mails datenschutzkonform nutzen

08/2021 Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder Stand 16.06.2021[56]:

Diese Orientierungshilfe behandelt ausschließlich die Risiken, die mit einer Verletzung von Vertraulichkeit und Integrität personenbezogener Daten verbunden sind … ausgehend vom Stand der Technik, den typischen Implementierungskosten und deren Verhältnis zu den Risiken einer Übermittlung personenbezogener Daten per E-Mail. Risiken, denen ruhende Daten, wie bereits empfangene E-Mails ... oder die durch eine Weiterverarbeitung wie z. B. automatische Weiterleitungen entstehen, werden in dieser Orientierungshilfe nicht betrachtet. Dieser Schutz muss abseits des Blickwinkels dieser Orientierungshilfe ergänzt werden durch Maßnahmen zum Schutz der beteiligten Systeme und zur Minimierung, Speicherbegrenzung und Zweckbindung der auf diesen Servern verarbeiteten Verkehrsdaten. (Auszüge)[2]

i) Dienstanbieterauswahl

Für die Verantwortlichen gilt eine Sorgfaltspflicht bei der Auswahl des E – Mail – Dienstanbieters. Dieser sollte hinreichend die Einhaltung der DS-GVO (u.a. kryptografische Algorithmen, Authentifizierung und Autorisierung der Gegenstelle) einschließlich technischer Richtlinien bestätigen bzw. garantieren. Orientierungsprofil ist die technische Richtlinie TR-03108 des BSI.[57]

ii) Anforderungen bei normalen Risiken für die Betroffenen

Eine obligatorische Transportverschlüsselung

(Protokolle: SMTPS, STARTTLS, TLS) nach dem Anforderungsprofil TR-02102 des BSI[58] gilt als Basisschutz bzw. Mindestanforderung. Einen unverschlüsselte Verbindung ist auszuschließen. Bei Entgegennahme von personenbezogenen Daten per E – Mail (z. B. über die Homepage) ist der Empfänger verpflichtet mit einem möglichst breiten Spektrum die Voraussetzungen für einen verschlüsselten Empfang zu gewährleisten bzw. zu schaffen. Die Verantwortung für die Übermittlung liegt beim Sender. E – Mail Signaturen sind zwingend zu prüfen und bei Fehlermeldungen an den Absender zurückzusenden.

Voraussetzung einer qualifizierte Transportverschlüsselung

Kryptografische Algorithmen und Protokolle nach dem Stand der Technik (BSI TR-02102[5]), DNSSEC – Signatur (Sicherheitsmechanismus zur Authentizität und Integrität) und authentifizierten, zertifikatbasierter Server

iii) Anforderungen bei hohen Risiken für die Betroffenen

Generell Transportverschlüsselung und Ende-zu-Ende Verschlüsselung.

Diese schützt nicht nur den Transport per E-Mail, sondern auch „ruhende Daten“ im Posteingang, bei Weiterleitung u. ä., wenn der Schlüssel dazu nur von Berechtigten vorgehalten wird. Aktuelle Standards lt. DSK: „S/MIME (RFC 5751) und OpenPGP (RFC 4880) i.d.R. in Verbindung mit PGP/MIME (RFC 3156). In welchem Umfang auf einzelne Maßnahmen verzichtet werden kann, hängt von den bestehenden Risiken, der konkreten Ausgestaltung des Übertragungsweges und ggf. getroffenen kompensierenden Maßnahmen ab.

Prüfroutine

Hinreichende Sicherheits- und Echtheitsprüfung von Zertifikaten oder öffentlichen Schlüsseln. Bei automatischem Austausch (z. B. Perfect Forward Secrecy) ist eine Verifizierung über einen anderen Kanal zwingend vorzunehmen. Eigene Schlüssel sollten mit hinreichenden Sicherheitsparameter erzeugt werden.

iv) Besondere Anforderungen bei Berufsgeheimnisträgern

Berufsgeheimnisse (z.B. Rechtsanwälte*innen, Ärzte*innen u.a.) stellen ein Indiz für eine hohes Risiko dar (Link: Erwägungsgrund 75 DS-GVO) und sind deshalb in ihrer Höhe für die Betroffenen besonders zu prüfen, unabhängig von anderen gesetzlichen Vorschriften (z.B. §203 StGB)[59]. Grundsätzlich gilt die Anforderungen für hohe Risiken einzuhalten, sofern sich nicht aus den konkreten Umstände ein normales Risiko ergibt.

v) Auf Schutzmaßnahmen verzichten?(??)

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat im Fazit eines 11-seitigen „Vermerks“ Stand April 2021[60] es wie folgt festgehalten:

> *Der Verantwortliche und der Auftragsverarbeiter haben die nach Art. 32 DSGVO (Sicherheit in der Verarbeitung) erforderlichen Maßnahmen zwingend umzusetzen und vorzuhalten. Betroffene Personen können in die Herabsetzung des nach Art. 32 DSGVO vorgesehenen Schutzniveaus allerdings bezogen auf ihre eigenen Daten im Einzelfall einwilligen, wenn die Einwilligung freiwillig im Sinne des Art. 7 DSGVO erfolgt. Dies setzt jedoch voraus, dass der Verantwortliche die nach Art. 32 DSGVO erforderlichen Schutzvorkehrungen grundsätzlich vorhält und der betroffenen Person auf Verlangen zur Verfügung stellt, ohne dass der betroffenen Person Nachteile dadurch entstehen.*

JA, Voraussetzungen sind:

1.) Der Verantwortlich muss die erforderlichen Schutzmaßnahmen in jedem Fall vorhalten!

2.) Die Bedingungen für eine Einwilligung nach Art 7 DSGVO sind zwingend einzuhalten!

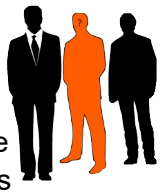
Zur Einwilligung

- Die Einwilligung ist in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so zu halten und von anderen Sachverhalten klar zu unterscheiden.
- Die Betroffenen sollten / müssen über die Möglichkeiten und den Risiken aufgeklärt sein.
- Die Freiwilligkeit ohne Zwang, also die Wahlmöglichkeiten muss dem gegebenen Umstand in größtmöglichen Umfang Rechnung tragen.
- Als Nachweis ist die Einwilligung eindeutig zu dokumentieren.

Aber Vorsicht!

Den Ausführungen des HambBFDI ist zu entnehmen, dass es ausschließlich im Interesse der Betroffenen liegen darf, da der Verantwortlich die erforderlichen Schutzmaßnahmen in jedem Fall zur Verfügung halten muss. Beispiele sind hier:
Zu einer unsicheren Datenverarbeitung darf nicht gezwungen werden, wer eine Onlinedienst nutzt, oder einen Arzt oder Rechtsanwalt seiner Wahl aufsuchen möchte. Auch höhere Alternativkosten oder verlängerte Bearbeitungszeiten sprechen gegen die Freiwilligkeit.

(x) Betriebsrat zum Datenschutz verpflichtet!



08/2021 Mit dem neuen §79a Betriebsverfassungsgesetz[61] wird der Betriebsrat auf den Datenschutz verpflichtet. Die Datenschutzbeauftragten sind über die jeweilige Meinungsbildung zur Verschwiegenheit verpflichtet. Verantwortlicher bleibt der Arbeitgeber und hat die Verarbeitungstätigkeiten in sein Verfahrensverzeichnis aufzunehmen. Es gilt die gegenseitige Unterstützungspflicht auch zur Einhaltung der Betroffenenrechte (z. B. Auskunftsersuchen). Das wird für manchen internen Datenschutzbeauftragten keine leichte Aufgabe.

(y) Auftragsverarbeitung

Mit der lange angekündigten und erwarteten Veröffentlichung der neuen Standardvertragsklausel für die Drittlandübermittlung durch die EU - Kommission[62] ist der zusätzlich veröffentlichte

„DURCHFÜHRUNGSBESCHLUSS DER KOMMISSION über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 DS-GVO und Artikel 29 der EU – Verordnung 2018 / 1725 für die Organe und Einrichtungen der EU (Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter in der EU / im EWR)[63]“

etwas, sagen wir: „untergegangen“.

i) Definition Auftragsverarbeitung

In einfachen Worten: „Jede Möglichkeit der Kenntnisnahme von personenbezogenen Daten in jedweder Form (digital, beleghaft u.v.m.), bei der Beauftragung eines Dritten zur Verarbeitung durch einen Verantwortlichen.“ Der Begriff und die Definition ergibt sich aus Art.4 Abs.2 und Art.28 Abs.1 DS-GVO, im Besonderen in Verbindung mit den Erwägungsgründen DS-GVO Nr.13, 18, 81, 95.

ii) Wann liegt eine Auftragsverarbeitung vor?

WENN beim Verarbeitungsprozess personenbezogene Daten verarbeitet werden
UND eine andere Stelle für die Erhebung oder Verarbeitung usw. verantwortlich ist (!)
DANN liegt eine Auftragsverarbeitung vor!

iii) Wann liegt keine Auftragsverarbeitung vor?

WENN die Verarbeitung lediglich im Zusammenhang mit einer Leistungserbringung steht und eine Direktverbindung zum Betroffenen erfolgt,
DANN liegt keine Auftragsverarbeitung wegen eigenem Rechtsgrund (Vertrag, Einwilligung) vor!

Beispiele: a.) Vermittlung oder Weiterleitung eines Auftrags zur Lieferung / Leistung (Onlineshop gibt dem Hersteller den Auftrag zur direkten Lieferung/Leistung an den Endkunden.
b.) Gemeinsame, getrennte Leistungserbringung als „gemeinschaftlich Verantwortliche“[64].

iv) Was ist bei einer Auftragsverarbeitung zu beachten?

Nach Art.28 (&29) DS-GVO gilt der Grundsatz: „Der Schutz reist mit den Daten!“ Der Auftragsverarbeiter muss geeignet sein, den Datenschutz und die Regeln einzuhalten, was vom Verantwortlich zu prüfen ist. Das schließt alle möglichen Unterauftragsverarbeiter mit ein, die auch nur im beiderseitigem Einvernehmen einbezogen werden dürfen (Abs.1, 2). Für die Verarbeitung ist zwingend ein Auftragsverarbeitungsvertrag abzuschließen (Abs.3). In diesem Vertrag wird die Einhaltung der Datenschutzregeln verpflichtend festgeschrieben. Weitere wesentliche Inhalte sind der Gegenstand und die Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen und Pflichten und Rechte des Auftragsverarbeiters und der Verantwortlichen, insbesondere konkrete Festlegung der Weisungs- und Kontrollbefugnis.

Wie einleitend beschreiben, hat die EU – Kommission dazu (genehmigte) Standardvertragsklauseln dazu veröffentlicht. Für den nicht öffentlichen Bereich finden Sie auf meiner Website (siehe Fußnote[65]) ein Vertragsmuster auf diese Basis.

v) Kurze Checkliste Auftragsverarbeitung

A. Kleine Checkliste der zu treffenden Regelungen und Inhalten bei der Auftragsverarbeitung			
❒	Gegenstand, Zweck, Art der Datenverarb.	❒	Dauer, Datenkategorien, Betroffenenkreis
❒	Datensicherheit (techn.--org. Maßnahmen)	❒	Weisungsgebundenheit
❒	Unterauftragsverarbeiter	❒	Informationspflichten
❒	Vertraulichkeit	❒	Unterstützung bei Transparenzpflicht
❒	Unterstützung bei Nachweispflicht	❒	Unterstützung zu Betroffenenrechten
❒	Rückgabe & Löschung	❒	Kontrollrechte (vor Ort, Nachweise)
❒	Informationspflichten (z.B. bei Verstößen)	❒	Weitere Punkte (Strafen, §88TKG usw.)

Bei vielen Unternehmen (z. B. Cloud – und Telekommunikationsanbieter) sind die Klauseln bereits in den Verträgen enthalten, oder stehen als Standard zum Abschluss im Netz zur Verfügung.

(z) TTDSG?!

10/2021 Das Telekommunikation – Telemedien – Datenschutz – Gesetz, in Kraft ab 01.12.2021. Wie das Bundesministerium für Wirtschaft und Energie zum Gesetzgebungsverfahren schreibt[66], werden hier die Bestimmungen zum Datenschutz aus dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) in einem Stammgesetz zusammengeführt. Die bisherige Lücke zur Regelung von behördlichen Auskunftsersuchen wird damit geschlossen. Die hier festgelegten Strafen sind auch nicht gerade „kleinlich“. In der EU befindet sich die ePrivacy – Verordnung zur Flankierung der DS-GVO und zur Ablösung der veralteten ePrivacy – Richtlinie unverändert in der Abstimmung. Weitere Regelungen zur Schnittstellenkommunikation, IoT, Wettbewerbsnutzung, Tracking, „End-to-End“ - Verschlüsselung u.ä. sind im Gespräch und deren Auswirkungen noch nicht absehbar. Einen zusammenfassenden, kurzen Überblick aus meiner Datenschutzbrille ist zu finden unter: https://www.volkerschroer.de/DSGVO/2021.10.07.TTDSG-kurzgefasst.pdf.

Spannend ist das Thema „Personal – Information – Management – System“, als ein sicheres Kontroll- und Verwaltungssystem des einzelnen Individuums mit der Entscheidungsgewalt, wann und mit wem Daten geteilt oder nicht (mehr) geteilt werden. Ein solches System würde z. B. die „Cookie – Banner“ erübrigen.

(aa) Fristablauf für Einwilligung (Werbung)?

10/2021 Zur Zeit „unentschieden“!

i) Urteile & Entscheidungen[67]

2010.04.08 OLG München, Entscheidung zu 17 Monaten: *„Es ist ... allgemein anerkannt, dass eine einmal erteilte Einwilligung mit Ablauf eines längeren Zeitraumes ihre Aktualität verliert … Damit lag zwischen der Einwilligung und Versendung der E-Mail ein Zeitraum von etwas mehr als 1 ½ Jahren. Damit hatte die Einwilligung, so sie denn erteilt worden war, jedenfalls ihre Aktualität verloren.“*

2016.10.05 AR Bonn, Entscheidung zu 4 Jahren: *„Bei einem solchen Zeitablauf kann nicht mehr von einer erteilten Einwilligung ausgegangen werden.“*

2018.02.01 BGH, Entscheidung zu Fristablauf: *„Eine zeitliche Begrenzung einer einmal erteilten Einwilligung sieht weder die Richtlinie 2002/58/EG noch §7 UWG vor. Hieraus ergibt sich, dass diese - ebenso wie eine Einwilligung nach §183 BGB - grundsätzlich nicht allein durch Zeitablauf erlischt.“*

2018.11.17 DatenSchutzKonferenz (Bund/Land): *Orientierungshilfe zur Verarbeitung von personenbezogenen **Daten für Zwecke der Direktwerbung** unter Geltung der Datenschutz-Grundverordnung (DS-GVO): „3.5 Die Zivilgerichte sehen bei erteilten Einwilligungen zur werblichen Kontaktaufnahme teilweise keine unbegrenzte Gültigkeit. … Einwilligung zur E-Mail-Werbung „ihre Aktualität verliert“ und deshalb insoweit keine rechtliche Grundlage mehr ist. … 4.8 Eine konkrete Frist hat der Gesetzgeber nicht vorgesehen. Entscheidend ist, ob aufgrund der Art der Geschäftsbeziehung noch eine Erforderlichkeit zur weiteren Nutzung der Daten für Zwecke der Direktwerbung von dem Verantwortlichen nachvollziehbar dargelegt werden kann.“*

ii) Fazit:

Fakt scheint nur, dass es eine Ablauffrist grundsätzlich (noch) nicht gibt. Aber, wurde z. B. die Einwilligung zu Werbezwecken mit einem Vertrag eingeholt und dieser ist gekündigt, dann wird es mit der „Darlegung der Nachvollziehbarkeit“ (DSK) schon schwierig, zumal es ja allein aufgrund des Kopplungsverbots (§ 7 Abs.4 DS-GVO) zu trennen ist (von Gewinnspielen mal ganz abgesehen). Nach Art.17 Abs.1 (a) besteht eine Löschpflicht, wenn Daten nicht (mehr) benötigt werden. Der Zweck für eine länger, ungenutzte Speicherung wäre also darzulegen. „Vorratsspeicherung“ entfällt damit. Praxis z. Zt. ist eine Erneuerung oder Löschung nach spätestens 2 „ungenutzten“ Jahren.

(ab)DSK zu Impfstatusabfrage [68]

10/2021 Die Datenschutzkonferenz (Bund/Länder) sieht für die generelle Impfstatusabfrage der Arbeitgeber keine gesetzliche Grundlage. Abfrage nur in Einzelfällen, z. B. Lohnersatz w/Quarantäne, oder besonderen Berufsgruppen nach dem IfSG (Krankenhaus, Pflege, Kindergarten u.ä.)

(ac)DS-GVO Hauptakteure

11 2021 ***Verantwortliche“*** sind natürliche oder juristische Personen, die allein oder gemeinsam über Zweck und Mittel der Verarbeitung entscheiden (Art.4 Nr.7 DS-GVO). Die Vertreter sind schriftlich zu bestellen (Art.4 Nr. 17 DS-GVO). Risiken und Haftung tragen ausschließlich die Verantwortlichen mit der Entscheidung.

„Auftragsverarbeiter“ sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten. Es besteht keine Verbindung zu den Betroffenen (Art.4 Nr. 8 DS-GVO) und gelten in Bezug auf diese Verarbeitungen als Verantwortliche (Art 28 Abs.10 DS-GVO).

„Gemeinsame Verantwortliche“ Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche (Art.26 DS-GVO). Ein Beispiel ist die Facebook (Meta) Fanpage (EuGH Nr. 81/18 v. 05.06.2018)[69].

„Datenschutzbeauftragte“ werden auf der Grundlage ihrer beruflichen Qualifikation und insbesondere des Fachwissens benannt (Art.37 Abs.5 DS-GVO). Ihre Aufgaben umfassen (nur) Unterrichtung und Beratung, Überwachung und Einhaltung, Beratung zu Folgenabschätzungen, Zusammenarbeit und Ansprechpartner für die Aufsichtsbehörden und Anlaufstelle für die Betroffenen. (Art. 39 Abs.1 DS-GVO) .

„weitere Beteiligte“: Art.4 DS-GVO (Nr.) Vertreter (17), Betroffene, Empfänger (9), Dritte (10), Drittland (ex EU), internationale Organisation (26)

(ad)DS-GVO, die Ausnahmen

„***Haushaltsausnahme“:*** Diese Verordnung findet keine Anwendung auf die Verarbeitung von personenbezogenen Daten (c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (Art.2 Abs.2 lit.c DS-GVO).

„Datenschutzbeauftragte“: Keine Pflicht zur Bestellung, sofern weniger als 20 Personen mit der Verarbeitung beschäftigt sind *und keine* geschäftsmäßige Verarbeitung zur Übermittlung, anonymisierter Übermittlung oder für Markt- oder Meinungsforschung *und keine* Datenschutz-Folgeabschätzung erforderlich ist. Es gilt die DS-GVO immer einzuhalten (§38 Abs.1 BDSG).

„Verfahrensverzeichnis“: Zum Verzicht auf ein Verfahrensverzeichnis für Kleinstunternehmen und Unternehmer sagt die Datenschutzkonferenz: „Es ist davon auszugehen, dass diese Ausnahmen nur selten greifen werden und vielfach das Erstellen eines Verzeichnisses von Verarbeitungstätigkeiten geboten ist[70]. Art.30 Abs.5 DS-GVO spricht zwar von weniger als 250 Mitarbeitern, ***es sein denn***, u. a. die Verarbeitung erfolgt ***nicht nur gelegentlich,*** z. B. das führen einer Kundendatenverwaltung, oder Lohnabrechnung, oder IT – Internet, E-Mail Protokollierung.

(ae)Was ist jetzt mit Fotos?

11/2021„Dr. Datenschutz“ hat dazu eine sehr anschaulichen Fachbeitrag des Zusammenwirkens der verschiedenen Gesetze mit der DS-GVO veröffentlicht[71]. Kurz zusammengefasst:

- ✔ Bei, mit ausreichender Auflösung, erkennbaren Personen auf Fotografien handelt es sich um personenbezogene Daten und zwar unabhängig ob Porträt (alt: Portrait) oder Gruppenaufnahmen. Bei digitalen Aufnahmen meist noch mit verbundenen Metadaten (Ort, Zeit u.ä.).
- ✔ Es Bedarf also einer **Einwilligung** (Mitarbeiterfotos, interne Organigramme, Homepage, Flyer u. ä.). Es geht auch mündlich oder durch konkludentes Handel, allerdings ist die Nachweispflicht im Bedarfsfall schwierig und in jedem Fall muss die Person auf Ihre Rechte (Auskunft, Widerspruch u.s.w.) hingewiesen werden. - **Oder –** Grundlage ist eine **vertragliche Verpflichtung** (z. B. Bewerbungsfotos, Zugangsfunktionen, Marketingverträge). **- Und - Bei Kindern** ist in jedem Fall die Einwilligung aller Erziehungsberechtigten einzuholen! **- Oder –** es liegt ein **berechtigtes Interesse** des Fotografen vor, sofern die Interessen des Betroffenen nicht überwiegen (!). Beispiele sind künstlerische oder dokumentarische Aufnahmen, wenn die Passanten nur „Beiwerk“ sind, oder bei geschlossenen Veranstaltungen, sofern die Bildern nur den Teilnehmern zur Verfügung stehen und nicht Dritten über Internet, Social – Media u. ä.
- ✗ Für rein persönliche, familiäre Zweck gilt die „Haushaltsausnahme“ nach Art2. Abs.2c DS-GVO.
- ✗ Ausnahmen gelten auch für das Medien- (RStV §9c) bzw. Kunstprivileg nach §23 KunstUrhG für die Bereiche: Zeitgeschichte, Örtlichkeiten (als Beiwerk), Teilnehmer an Versammlungen oder Veranstaltungen und höheres Interesse der Kunst, sofern nicht die berechtigten Interessen der Betroffenen überwiegen.

(af) Reicht die Datenschutzerklärung Webseite auch für den Betrieb?

*11/2021*Eine Datenschutzerklärung, also die Information an den/die Betroffenen hat immer vor Datenerhebung zu erfolgen. Der Hinweis auf die Veröffentlichung auf der Website reicht nicht aus, da diese eben nur bei der (und für die) Nutzung der Website gilt. Projekt29[72] berichtet von einer aktuellen Beschwerde beim BayLD eines Patienten, da er in der Arztpraxis nur auf die Website – Erklärung verwiesen wurde. Aushang oder Informationsblatt ist in jedem Fall vor Ort erforderlich.

(ag)3G am Arbeitsplatz

*12/2021*Da war was … Infektionsschutzgesetz (§28 IfSG)[73] und Datenschutz. Eine kurze Zusammenfassung und Anleitung für einen schlanken Ablauf im Sinne der Gesetze IfSG, DS-GVO & BDSG hatte ich vorab auf die Website mit Pflichtinformation gestellt. Link „3G am Arbeitsplatz – DS-GVO & IfSG“.

(ah)Wer fällt unter das TTDSG?

*12/2021*Das Gesetz sagt in §2 Abs.(2) Nr.1 TTDSG *„Anbieter von Telemedien jede natürliche oder juristische Person, die eigene oder fremde Telemedien erbringt, an der Erbringung mitwirkt oder den Zugang zur Nutzung von eigenen oder fremden Telemedien vermittelt“* und in §1 Abs.(3) TTDSG *„Diesem Gesetz unterliegen alle Unternehmen und Personen, die im Geltungsbereich dieses Gesetzes eine Niederlassung haben oder Dienstleistungen erbringen oder daran mitwirken oder Waren auf dem Markt bereitstellen. § 3 des Telemediengesetzes bleibt unberührt. (d. h. das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.)“*

i) Einschätzung

Also auch jeder und jedes Unternehmen, dass Inhalte (Video, Audio, Informationen, Angebote u.s.w.) über Telemedien zur Verfügung stellt, ohne dass ein Telemedien-Service-Provider in die Kontrolle oder Verbreitung der Inhalte involviert ist.

ii) Ein Vorteil

Nach den Auslegungen gehören Anwendungen / Plattformen zur Kommunikation und Kollaboration (z. B. Teams, ZOOM & Co.) zu den Telekommunikationsdiensten, denn ein großer Teil der Datenverarbeitung findet in deren Verantwortung statt. Ein Vertrag über die Auftragsverarbeitung für die Kommunikationsmedien ohne die Zusatztools entfällt eigentlich damit. Bis zur allgemeinen Anerkennung wird es noch etwas Zeit brauchen.

iii) Ein Nachteil[74]

Durch (*§3 Abs.2 Nr.2 TTDSG „ganz oder teilweise geschäftsmäßig angebotenen Telekommunikations-diensten“*) bleibt es bei der Einhaltung des Fernmeldegeheimnisses bei der privaten Nutzung geschäftlicher Kommunikationsdienste, ob vereinbart oder geduldet. Jetzt eben geregelt in §3 TTDSG statt §88 TKG[alt.], zumal die Einhaltung der DS-GVO bleibt. Eine Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis ist nicht zwingend da Gesetz. Wegen der erheblichen strafrechtlichen Risiken mit Blick auf die Fürsorgepflicht aber hilfreich. Es bleibt bei den alten Prioritäten: ☺ verbieten ☹ regeln 😉 dulden. Bei Bedarf stelle ich gerne ein Muster „Dienstver-einbarung“ zur Verfügung.

iv) Cookies, dass kann doch nicht so …

… schwer sein! Nach Art.4 Abs.1 Nr.11 DS-GVO ist eine Einwilligung eine „*in informierter Weise und unmissverständlich abgegebene Willensbekundung*“. Es muss also klar und deutlich benannt werden, wofür die Daten verwendet werden. Braucht es dazu eine 33-seitige Orientierungshilfe[75] der DSK? Drei wesentliche Dinge, die mir im Dokument aufgefallen sind:

1.) Der Button: „Allen zustimmen“ erfordert zwingend deckungsgleich „nur notwendige Cookies“
2.) Transparent bereits im Banner:“Wer,Was,Warum“ und nicht über Link „Datenschutzerklärung“
3.) Zu Einwilligungen zu Drittlandtransfer (von Schriften, Skripte, Maps, Social- & Media) gibt es keine „Dauergenehmigung“ (siehe hierzu Seite 33 Ende letzter Absatz[3])

(3) Zur Datensicherheit:

(a) Der „kleine Helfer“

01/2021 Das Bundesministerium für Wirtschaft und Energie hat die Einrichtung einer Transferstelle für IT-Sicherheit im Mittelstand beschlossen. Diese soll ein bundesweites Angebot für kleine und mittlere Unternehmen mit zielgruppengerechten, passgenauen Maßnahmen bereitstellen, verbunden mit der Vermittlung lokaler Fachkräfte / Unternehmen. Der entwickelte Sec-o-Mat ermittelt an Hand ausgewählter Fragen einen Aktionsplan (und bietet lokale Fachkräfte / - unternehmen zur Unterstürzung an), zu finden unter dem Link in der Fußnote[76].

(b) Home Office – Charter of Trust

02/2021 Die aktuelle COVID 19-Krise hat zu einem exponentiellen Anstieg der Zahl der Menschen, die von zu Hause aus arbeiten - geführt, um die öffentliche Gesundheit zu schützen. Gleichzeitig besteht ein erhöhtes Risiko in Bezug auf die Cybersicherheit. Um die Sicherheit zu verbessern haben sich viel deutsche Großunternehmen (Telekom, Cisco, IBM, TÜV-Süd u.a.) auf Initiative der Siemens AG zusammengeschlossen und „Charter of Trust“ gegründet[77]. Von dort 8 Tipps (eigentlich generell zu beachten) für sicheres Home-Office:[78]

✔Nehmen Sie nur Geräte und Informationen mit, die unbedingt notwendig sind	✔Schützen Sie Ihr Heimnetzwerk und kommunizieren Sie über sichere Verbindungen
✔Halten Sie die Software auf allen Ihren Geräten auf dem neuesten Stand	✔Schalten Sie sprachgesteuerte Smart-Geräte an der Arbeitsstation aus und decken Sie die Webcam ab, wenn Sie sie nicht verwenden
✔Mischen Sie nicht den persönlichen und geschäftlichen Gebrauch von Geräten	✔Identifizieren Sie proaktiv alle Teilnehmer an Online-Meetings
✔Melden Sie sich ab, wenn Sie Ihre Geräte nicht mehr verwenden, und bewahren Sie sie sicher auf	✔Seien Sie äußerst vorsichtig bei verdächtigen E-Mails oder Anhängen, insbesondere wenn Sie den Absender nicht kennen

(c) BSI „IT – Bedrohungslage ROT“[79]

03/2021 Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrechterhalten werden" – das ist die aktuelle Einschätzung der Situation durch das BSI. Ursache sind die Sicherheitslücken in Microsoft Exchange, für die der Hersteller in der Nacht zum Mittwoch, dem 3. März, Out-of-Band Updates veröffentlicht hat.

Das Sicherheitsupdate sollte so schnell wie möglich installiert werden. Wie ein IT-Experte der BREDEX GmbH auf dem BSI – IT – Grundschutztag am 17.03.2021 berichtet, ist das Update unbedingt und nur manuell zu installieren, da viele Einstellungen auf Standard gestellt werden, das

System unter Last gestellt wird und eine Deinstallation nicht möglich ist. Es erfordert somit die Aufmerksamkeit der Administratoren. Das BSI stellt eine „Cyber Sicherheitswarnung“ und „Microsoft Exchange Schwachstellen Detektion und Reaktion“[8] als Prüferfordernisse zur Verfügung.

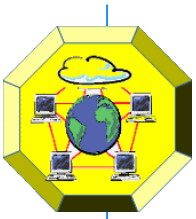
(d) Schlechte Zeiten für Social Media (Schadenersatz?)

04/2021 Die Betroffenheit von Social Media durch abgreifen von Nutzerdaten hat golem.de[80] gut zusammengefasst

✖ Clubhouse 1,3 Millionen	✖ Linkedin: 500 Millionen	✖ Facebook / Whatsapp 533 Mio.

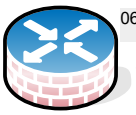
Diese und ähnlich sorglose Anbieter bleiben leider ein Einfallstor für die Verteilung von Spam, Vieren, Trojaner, Identitätsdiebstahl und das Ausspionieren von Beziehungen und Verbindungen zum Angriff auf Unternehmen und Organisationen. Ein vorsichtig, zurückhaltender Umgang ist, wenn nicht vermeidbar, angebracht. Die Europäische Gesellschaft für Datenschutz (EuGD) strebt eine *Sammelklage auf Schadenersatz* nach DS-GVO Art.82 gegen Erfolgsprovision lt. FOCUS[81] an.

(e) SiSyPHuS



05/2021 Diese Bezeichnung drückt es m. E. korrekt aus und ist für den ISB (Informationssicherheitsberater) bzw. den IT – Leiter oder Dienstleister bestimmt. Mit dem Projekt SiSyPHuS Win10 (Studie zu Systemintegrität, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10) lässt das BSI Sicherheitsanalysen der sicherheitskritischen Funktionen in Windows 10 durchführen sowie darauf aufbauend passende Härtungsempfehlungen erstellen (Link in der Fußleiste [82])

(f) IT – Sicherheitsgesetz 2.0 (IT - Sig 2.0)[83]



06/2021 Folgende Neuerungen sind laut BMI[9] mit dem IT – Sig 20 verbunden. Das Bundesamt für Sicherheit in der Informationstechnik *(BSI) wird Deutschlands zentrale Cybersicherheitsbehörde* und ist nach dem Cyber Security Act der EU nationale Stelle für Sicherheitszertifizierung und Konformitätsbewertungsstellen mit Auskunftsrecht, legt die Definition von „neuestem Stand der Technik“ fest und darf Sicherheitsrisiken detektieren. Damit ist das „Angreifen“ von Unternehmen zur Entdeckung von Schadprogrammen, Sicherheitslücken und -risiken unter diesen Umständen erlaubt. Zur *Sicherheit der Mobilfunknetze* müssen Betreiber künftig vorgegebene, hohe Sicherheitsstandards erfüllen, mit der Möglichkeit des BSI den Einsatz von kritischen Komponenten zum Schutz der öffentlichen Ordnung und Sicherheit zu untersagen Im Rahmen des neuen *Verbraucherschutzes* soll ein neues, freiwilliges IT – Sicherheitskennzeichen eingeführt werden. Das BSI wird für die Prüfung, Vergabe und Überprüfung (mit Möglichkeit der Aberkennung) zuständig. *Unternehmen mit kritischen Infrastrukturen und im öffentlichen Interesse* (KRITIS+) müssen künftig bestimmte Sicherheitsmaßnahmen erfüllen, z. B. Intrusion Detection System (IDS) zur Angriffserkennung, Auswertung von Log-Dateien, verpflichtende Abgabe von Störmeldungen oder die Ausarbeitung von Präventivmaßnahmen und Reaktionsplänen (Business Continuity Planning; Desaster Recovery Szenarien). Deutlich erhöhter *Bußgeldrahmen* gemäß §14 Abs (5) mit bis € 2 Mio. und mit dem dortigen Verweis auf OWiG §30 Absatz 2 Satz 3 auf bis zu € 20 Mio.

(g) Hochrisikogruppe: Social – Media – Nutzer?

06/2021 Projekt 29 berichtet[84] von einer neue Studie der TU Darmstadt und IT - Seal GmbH, wonach aktive Social – Media - Nutzer deutlich verwundbarer gegenüber Cyberangriffen sind als Nicht (so aktive) Social Media Nutzer. Zitat:

Aktueller Job, Ausbildung, Zertifikate, Hobbies und Kollegen – All diese Daten und Informationen aus sozialen Netzwerken stehen in vielen Fällen frei zugänglich im Internet zur Verfügung. Cyberkriminelle nutzen diese Informationen, um darauf aufbauend unter anderem gezielte Phishing-Mails zu erstellen, die bei ihren Opfern, ausgestattet mit realen Informationen, eine hohe Glaubwürdigkeit erzeugen.
Die Antwort ist eindeutig: “Nutzer von Sozialen Medien sind als Hochrisikogruppen bezüglich Phishing Angriffe anzusehen”, erklärt Anjuli Franz von der TU Darmstadt. Diese Forschungsergebnisse besitzen vor dem Hintergrund der kürzlichen Daten - Leaks von LinkedIn und Facebook, mit je einer halben Milliarde veröffentlichter Nutzerprofildaten, eine besondere Relevanz.

Meinung: Sollte ich mich jetzt von Facebook, Google, Skype & Co abmelden? „*Na ja … Vorsicht mit den Inhalten ist sicherlich angebracht und ein paar Schutzmaßnahmen zur digitalen Selbstverteidigung, wie auf young data – open & safe*[85] *sind sicherlich angebracht.*“

(h) BSI – Neuheiten

07/2021 Das Bundesamt für Sicherheit in der Informationstechnik hat neue, informative Seiten für Interessierte eingestellt, unterteilt nach Allgemein, Büro, Remote, Server, Netzwerke, Steuerung, Cloud, Webanwendungen und Faktor Mensch. Hier der LINK für Interessierte.

(i) Angriffsziel deutsche Wirschaft – Rekordschaden[86]

08/2021 Wie der Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien (Bitkom) mitteilte, sind die Schäden aus Cybercrime auf den Rekordwert von 223 Mrd. € (+216%) gestiegen. Die Umfrage umfasste mehr als 1.000 deutsche Unternehmen quer durch alle Branchen, davon wurden 88% (v.J. 75%) zum Angriffsziel. Einfallstor ist zum einen das Social – Engineering (Manipulation von Beschäftigten und Leitung) und zum anderen das Home – Office. Dort kam es bei der Hälfte der Angriffe auch zu Schäden. Und es geht nicht nur ums Geld, Kommunikationsdaten und geistiges Eigentum stehen auch im Fokus der Angreifer.

(j) Zweifel: System befallen?

Gelegentlich scheint das eigene System eigenartige Vorgänge durchzuführen. Zweifel kommen auf, ob nicht ein „Befall“ vorliegt. Microsoft bietet ja unter seinen DOCS „Windows Sysinternals“ Systemwerkzeuge an (*Abteilung von Microsoft, gegründet und geführt von Mark Russinovich, Technischer Direktor Microsoft Azure*)[87]. Mit den für und von Profis entwickelten Werkzeugen kann ich als „unbedarfter“ Windowsanwender durchaus eine erste Analyse vornehmen. Unter den kostenlosen Werkzeugen befindet sich das Programm „Process Explorer“[88] zum Download oder Live – Ausführung (ZIP – Datei, entpacken, direkte Ausführung). Neben den Statistiken zur Auslastung, fand ich weitere, einfache Analysefunktionen:

(a) Verifizierung des Datei Herstellers (Option:Verify Image Signatures)
(b) Online – Virus – Prüfung bei über 70 Anbietern[89] (Option: Check VirusTotal.com)

Jetzt bedeutet es nicht, wenn eine Signatur nicht geprüft werden kann, oder einer von 70 Antivirusanbietern anspringt, dass gleich ein Befall des Systems vorliegt. Aber, es lohnt sich zu prüfen, zu welchem Programm gehört die Anwendung (Programmpfad über „Mouseover“) und wann wurde diese mit welchem Programm installiert. Für Interessierte zu den vielfältigen Funktionen gibt es ein Video von Mark Russinovich (Tech Ed[90]). HINWEIS: Bei Firmen Hard- & Software immer erst an die Administration wenden (!), denn es kann ja noch andere, möglichen Gründe geben.

(k) BSI Lagebericht – Alarmstufe R O T

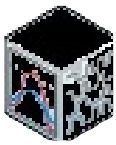
10/2021 Das Bundesamt für Sicherheit in der Informationstechnik hat seinen Lagebericht veröffentlicht (100 Seiten, Berichtszeitraum 06/2020-05/2021)[91]. Nur wenige TOP – Nachrichten aus dem Bericht:

- Stetig rasant steigende Anzahl von Angriffen und neuer Varianten von Schadsoftware (+22% p.a.)
- Cyber - Kriminelle suchen vermehrt den indirekten, einfacheren Weg über Dritte, um größere Ziele anzugreifen. In Wertschöpfungsketten wird zunehmend der Angriff über Zulieferer, Subunternehmen und/oder Mitarbeiter gesucht (sekundär Ziele), bei gut geschützten Zielobjekten.
- Stark zunehmend erfolgen Erpressungen mit *angeblichem* Videomaterial des Opfers, das dieses beim Besuch einer Webseite mit pornografischen Inhalten zeige, mit der Drohung es zu veröffentlichen.

(l) Wie Hacker die Psyche entschlüsseln [92]

11 2021 Awareness - Poster „Psychotricks und Phishing-Maschen“ des BSI zum Download. „Ein“ Poster zum Aufhängen, dass übersichtlich die Formen des Hacking vor Augen führt und hält.

(m) Gefahr Deepfakes (mit KI)



11/2021 Eine Gefahr für Firmen (z. B. „wenn der CEO persönlich anruft“), Individuen und auch der Demokratie, wie t3n berichtet[93]. Das ergibt sich alleine schon aus der Definition in einer EU – Studie:

„Deepfakes im Sinne der Studiendefinition sind zunehmend realistisch wirkende Fotos, Audios oder Videos, in denen Personen mithilfe von Systemen künstlicher Intelligenz in neue Kontexte gestellt werden. Dabei könne ihnen etwas in den Mund gelegt werden, das sie nie gesagt haben. Ebenso könnten sie an Orten auftauchen, an denen sie nie gewesen sind, oder Dinge tun, die sie nie getan haben.“

(n) Log4j: „Undankbarkeit ist der Welt Lohn“ (?!)[94]

Moderne, fragile, digitale Infrastruktur von xkcd.com unter (CC BY-NC 2.5)

12/2021 **Log4j ist** eine Art Protokollierung über die Aktivitäten in einer Software um Fehler zu finden und ggf. als rechtlicher Nachweis zur Nutzung. Die Open – Source - Software (OSS) wurde von einem „Freizeit – Programmierer“ ohne Dankbarkeit zu erwarten erstellt. Ohne Dank, geschweige denn Geld, haben gut bezahlte Techniker den Source - Code in ihre kommerziellen Programme übernommen und alle schimpfen jetzt auf die Programmierer.
Der Fehler war die Möglichkeit neben der Protokollierung auch unbemerkt (schadhafte) Befehle zu schreiben und diese auszuführen. Stand 15.12.2021 ist der Fehler mittlerweile behoben!

Open – Source – Software ist nicht kostenlos, sondern bietet u. a. den Vorteil für jeden, nach Nutzen und Geldbeutel, die Programmierung und Weiterentwicklung zu unterstützen.

Die Vorteile von OSS überwiegen m. E. Durch die freie Verfügbarkeit und die Verpflichtung zur Weitergabe des Quelltextes ist sie herstellerunabhängig, mit möglichst vielen Systemen kompatibel, vielfältig, flexibel, bietet jedem die Qualität und Sicherheit zu überprüfen, um nur einige Vorteile zu nennen. (Beispiele: Linux, Github, MySQL, LibreOffice, Cryptomator)
Eine Unterstützung der Projekte durch Beteiligung oder Spende hilft beiden Seiten (Win – Win).

(o) Bewusstsein & Aufmerksamkeit

12/2021 Auf Wunsch habe ich das „Awareness – Poster“ des BSI[95] (W*ie Hacker die Psyche entschlüsseln … und wie man sich schützt*) mit mehr s/w statt grün/gelb zum farbschonenderen Druck erhellt und steht hier als <PDF – LINK> zum Download zur Verfügung. Die Auflösung reicht auch für einen guten A3 oder eines 2*A4 - Ausdruck.

(4) Zu angrenzenden Themen

(a) Clubhouse Hype

01/2021 Clubhouse ist eine Audio-App, bei der die Anwender Gesprächen wie bei einem Live-Podcast zuhören oder sich aktiv an Diskussionen beteiligen können. Im Gegensatz zu Netzwerken wie Twitter kann man Beiträge nicht schriftlich kommentieren oder „Likes“ vergeben. Der Dienst ist derzeit zwar nur auf Apple – Geräten zu nutzen und „Einlass“ erfolgt nur auf Einladung, wofür teilweise bis zu 50€ wohl gezahlt werden. Trotzdem hat der Dienst in Deutschland bereits Telegram von Platz 2 verdrängt. Ein gegebener Datenschutz ist auch hier sehr fraglich, wie die saarländische Aufsichtsbehörde gegenüber der Tagesschau erklärt. Die klassischen 3 Schwerpunkt sind: 1.) Zugriff auf Kontakte, 2.) unklare Datenschutzregeln und 3.) US – Unternehmen ohne rechtliche Vertretung in der EU[96]. Erste Erfahrungsbericht von Social – Media - Profis (ICON)[12] . Abmahnung durch Bundesverband Verbraucherzentrale laut Handelsblatt. [97]

(b) Mittelstandsschreck „Ransomware“

01/2021 Wie die Süddeutsche Zeitung berichtet, liegt die Quote eines Ransomware – Angriffes in Deutschland laut Umfrage von Crowdstrike bei 60%. Der Branchenverband Bitkom ermittelt einen Schaden in 2019 durch Cyberkriminalität von mehr als 100 Milliarden Euro[98].

(c) TKG, TMG, TTDSG & TKModG

02/2021 Nein, es ist keine Neuauflage des Songs „MfG“ der Fantastischen4. Das Telekommunikationsgesetze (=TKG, der Regelung des Wettbewerbs in der Telekommunikation), wie das Telemediengesetz (=TMG, als zentrale, rechtliche

Rahmenbedingungen für das Internet / Medien) enthalten unterschiedliche Anweisungen zum Datenschutz. Der Schutz der Privatsphäre soll im Einklang mit der DS-GVO im neuen Telekommunikation – Telemedien – Datenschutz – Gesetzt (=TTDSG) vereinheitlicht zusammengeführt werden. Gleichzeitig soll das Telekommunikationsgesetz modernisiert werden (=TKModG)[99].

Positiv aus dem vom Bundeskabinett am 10.02 beschlossenen Referentenentwurf[100] ist z. B. die Einschränkung der grundsätzlichen Einwilligung des Betroffenen nach DS-GVO wie folgt:

> *„Das gilt nicht für solche Tätigkeiten, die nach Artikel 5 Absatz 3 der E-Privacy-Richtlinie technisch erforderlich sind, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.“ (Seite 41 siehe Link[7])*

und z.B. eine klarstellende Regelung zum „Digitalen Nachlass“ wie folgt:

> *„§ 4 dient der Klarstellung und soll sicherstellen, dass das Fernmeldegeheimnis und der Grundsatz der Vertraulichkeit der Kommunikation nicht den Endnutzer und Personen, die an seine Stelle treten, in der Wahrnehmung ihrer Rechte beeinträchtigt.“ (Seite 36[7])*

(d) Wenn Datenschutz zur Ausrede wird!

03/2021 Der Tagesspiegel berichtet in einem Kommentar, sicherlich beispielhaft für viele Vorgänge und Äußerungen, an Hand von Aussagen von Schäuble und Spahn, wie der Datenschutz als Ausrede benutzt wird.[101]

i) ZU VIEL:

Wolfgang Schäuble im Fernsehen: „*Ich finde, wir hätten mit der Corona- App sehr viel mehr erreichen können, wenn wir in der Frage Datenschutz in der Abwägung der verschiedenen Grundrechte ein bisschen besser balanciert gewesen wären*“. Also: Zu viel Datenschutz hat es verbockt.

ii) ZU WENIG:

Wolfgang Schäubles Sprecher zur Veröffentlichung der Liste von Jens Spahn über Abgeordneten - Empfehlungen von Maskenherstellern: „*Abgeordnete haben nach einschlägiger Rechtsprechung ein berechtigtes Interesse an der Vertraulichkeit von personenbezogenen Daten, die von der Freiheit des Mandats geschützt sind. Solche Daten dürfen daher nur in eng begrenzten Ausnahmefällen herausgegeben werden*“ Also: Eine Veröffentlichung wäre zu wenig und gegen den Datenschutz.

iii) Oder noch anders:

Hier möchte ich ergänzen, dass öfter der Datenschutz vorgeschoben wird, obwohl es nicht am Datenschutz liegt. Als Beispiel siehe Punkte 2 (b), bei dem es wohl am mangelndem IT-Schutz gemäß IT – Grundschutzkompendium des BSI[102] gelegen hat.

(e) Datenschutzverletzung und die Kunden sind weg (Umfrage)

03/2021 Die Wirtschaft Woche Bericht zu einer Umfrage (Okta Digital Trust Index durch YouGov) unter 13.000 Büroangestellten, davon 2.000 aus Deutschland, das bei einer Datenschutzverletzung (=Mißtrauen) 45% die Produktnutzung dauerhaft einstellen, 43% ihr Konto löschen und 33% die App gleich ganz löschen. Wenn das kein Argument für Datenschutz und Datensicherheit ist!

(f) MS - Productivity Score[103]

03/2021 Auch Microsoft ist es wohl aufgefallen, dass der vom Arbeitgeber ermittelbare Produktivitätswert aus dem Nutzungsverhalten der User / Mitarbeiter nicht den gesetzlichen Regelungen hier entspricht.

(g) Europas Datenschatz brennt am Rhein

03/2021 Wie die Frankfurter Zeitung berichtet, kam es zu einem verheerenden Brand bei Europas größtem Cloud - Anbieter OVH (5. Etage, 12.000 Server). Damit waren mal gleich 3,6 Millionen Netzseiten und 464.00 Domains weg, manche wohl für immer bis zum Neuaufbau. „*Nun könnte man das als einen spektakulären Unfall ohne fatale Folgen abtun, wenn die Daten tatsächlich, wie es die Cloud - Rhetorik nahelegt, anderswo gespeichert und über andere Data Center weiterhin abrufbar wären. Das ist technisch auch möglich – aber offenbar hatten etliche Kunden aus Kostengründen auf derartige Sicherheitsnetze verzichtet*“.[104]

(h) Schufa „Check Now“

03/2021 Mit einer Freigabe zur Einsicht in die Kontoauszüge hat die Schufa Kunden in einem Test- / Pilotprojekt „Hilfe“ angeboten, um einen schlechteren Score möglichst zu verbessern. Abgesehen von Nachteilen, die Verbraucherschützen sehen, stehen dort auch viele andere, personenbezogen Daten[105]. Jetzt titelt die Südeutsche zwar „*Schufa stampft umstrittenes Projekt ein*“[106]. Beim Lesen des Artikels wird aber klar, das Projekt wird „nur“ umbenannt, bei der Schufa – Tochter Finapi konzentriert („*in der Branche üblich*“?) und der Ablauf durch Vorabinformation und freiwillige Entscheidung zur Weitergabe an Dritte geändert. Fazit: Gut, wer es nicht braucht.

(i) Gegensätze?

i) Cybersicherheit: Deutschland auf Platz 1 [107]

Deutschland zählt zwar nicht unbedingt zu den innovativsten Ländern, aber ist bei der Cybersicherheit auf Platz 1. Dies zeigt eine Umfrage von NordVPN in 192 Ländern bei gut 48.063 Befragten. Die Stärken liegen bei App – Berechtigungen, Passwörtern, Umgang mit „Fishing“ Anzeigen auf Plattformen und mit E – Mails von Banken oder Unbekannten. Ausbaufähig sind die Stärken beim Umgang mit Sicherheitseinstellung für mehr Privatsphäre, dem Wi-Fi Netzwerk, IoT – Geräten und dem Lesen von Nutzungsbedingungen sowie der Sammlung von Metadaten durch die Internet - Provider.

ii) BKA: Cybercrime Bundeslagebild 2020 [108]

05/2021 Sehr verständlich und kurzweilig (mit Thriller – Charakter und das für einen Behördenbericht) wird für die Gefahren sensibilisiert. „*Kriminelle haben doch an mir kein Interesse! (?)*“ DOCH, haben sie! (Seite 9): „*Die Opfer erkennen ihre Betroffenheit nicht (z. B. bei Diebstahl ihrer Identität bei einem Online-Shop). Die von ihnen eingesetzten technischen Geräte werden unbemerkt zur Begehung von Cybercrime - Straftaten missbraucht (z. B. bei Nutzung infizierter PCs oder Router als Teil eines Botnetzes zur Ausführung von DdoS – Angriffen).*“ Digitale Identitäten sind übrigens eine beliebte Handelsware im Darknet (Seite 12 Underground Economy Cybercrime – as – a – Service). Fallbeispiel Malware – Ausnutzung einer Schwachstelle zur Platzierung von Kryptominern auf Systemen in einzelnen Ämtern (Seite 20). Die Wertschöpfungskette: Ransomeware, von der Programmierung über die Erpressung zum Lösegeld (Seite 24 Abb. 26) in Verbindung mit den 9.Säulen der Cybercrime „Lieferketten“ (Seite 45/46). **Fakten sind:** →Täter sind global vernetzt, agieren zunehmen professioneller und benutzten Aktuelles (Corona) als Narrativ. →Verschlüsselungstrojaner bleibt Bedrohung für Wirtschaft und Öffentlichkeit. →Die Underground – Economy wächst und mit ihr die Angriffe.

Abb. 1: (Cybercrime Bundeslagebild, Bundeslagebild 2020, Seite 3)

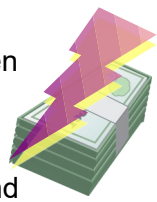
Fazit: LESEEMPFEHLUNG, Sensibilisiert für die Gefahren und ist leicht zu lesen.

(j) BigBrother – Awards 2021[109]

06/2021 Der BigBrother – Award (oder Datenkraken Oscar) ist ein internationales Projekt in 19 Ländern. Ein diesjähriger Preisträger ist das (Impf-) Terminvermittlungsportal für Ärzte der Doctolib GmbH. Mit diesem Portal werden unter Missachtung der ärztlichen Vertraulichkeit die Daten von zigtausenden Patienten/innen verarbeitet. Weitere Preisträger über den Link in der Fußzeile.

PS - t3n: Der Terminvergabe - Dienstleister Doctolib hat die Suchanfragen besorgter Patientinnen und Patienten per URL-Weitergabe mit Facebook und Outbrain geteilt.[12]

(k) Angriffsstrategien auf Finanzabteilungen



07/2021 „Finance & der Treasurer“ haben 4 + 1 der häufigsten Betrugsstrategien auf Finanzabteilungen zusammengetragen[110]:

i) Fake President,[111]

auch Chef-Betrug oder CEO/CFO - Fraud bezeichnet. Über öffentliche Quellen, Social – Media und gefälschte Anrufe werden Organisationen und Personen ausgespäht. Vertrautheit wird mittels falschen Anrufen, E-Mails zu Geburtstagen, Beförderungen u. ä. oder mit fiktiven Rechtsanwälten und Wirtschaftsprüfer per Telefon oder Videokonferenz hergestellt. Zu einem „geeigneten

Zeitpunkt“ (z. B. Freitagnachmittag, M&A Prozess) mit geringer Personalbesetzung werden Mitarbeiter als *„einzige, vertrauensvolle Person“* unter Druck gesetzt, eine dringende, eilige und wichtige Zahlung zu veranlassen. Dazu werden auch gut gefälschte E-Mails und / oder Verträge zugesandt. Laut FBI 20.000 Fälle in 2018 mit Schäden von 1,2 Mrd. US$. Die einzelnen Beträge variieren je nach Finanzkraft des Unternehmens.

ii) Payment Diversion

Änderung der Kontoverbindungen der Lieferanten. Früher vornehmlich per Brief oder Telefon, heute vermehrt über im Vorfeld abgefangene und gefälschte E-Mails oder Änderung im System über einen gehackten Zugang. Der Betrug fällt meist erst mit der ersten Mahnung auf.

iii) Goods Diversion

Die gleiche Masche wie bei Payment Diversion, nur werden hier die Waren umgeleitet. Gerne wird im Vorfeld auch eine echte Bestellung zur Vertrauenserschleichung durchgeführt.

iv) Ransomeware

Die in letzten Zeit gehäuft auftretende Erpresser – Software. Der meist über E-Mails, Hardware (USB-Stick) oder dem Netz eingeschleuste Trojaner verschlüsselt das ganze System. Zur Entschlüsselung wird ein Betrag erpresst. Der Treasurer bietet ein Checkliste „Erste Schritte“ an.

v) Umgekehrter Scheckbetrug

Hier wird ein ungedeckter Scheck zur Gutschrift „Eingang vorbehalten“ auf dem Firmenkonto eingereicht. Zwischen Vorbehaltsgutschrift und endgültiger Einlösung wird bei der Firma eine Überzahlung angemahnt mit der dringenden Bitte, diesen Betrag zurückzuüberweisen.

Ein Schutzkonzept sollte auch regelmäßige Sensibilisierung aller Beteiligten enthalten.

(l) Auch Cyberkriminelle „zoffen“ ums Geld

08/2021 Vom BKA wissen wir, dass Cybercrime as Service unterschiedliche „Lieferanten“ einbindet. So berichtet heise-online[112] von einem „unzufriedenen Angreifer“, der aus Frust über den geringen Anteil aus der Geldwäsche seine „minutiöse Gebrauchsanweisung“ für einen Ransomware - Angriff veröffentlichte. *„Die Conti Ransamware ist eine der aktivsten Verschlüsselungstrojaner“*. Neben der Infrastruktur, Tools und Anleitungen fand ich als kein IT – Forensiker bemerkenswert: Die Anleitung war auf Russisch / selbst für Laien verständlich / Lösegeldhöhe abhängig von der zuvor ausspionierten Umsatzhöhe / Anleitung zur Informationsbeschaffung über Social – Media zur Kompromittierung des Systems über den Menschen / Expliziter Hinweis auf deutsche „Domänen-Admins“ statt „Domain-Admins“. Wir sind also eindeutig im Visier der kriminellen Schattenindustrie

(m) Telefonwerbung ab Oktober

09/2021 Der Bundestag hat am Donnerstag, 24. Juni 2021, den Gesetzentwurf „für faire Verbraucherverträge“ (19/26915)[113] angenommen (Bundesgesetzblatt Nr. 53 vom 17.08.2021[114]). Zur „Einwilligung in Telefonwerbung“ auf Seite 9:

(1) Wer mit einem Telefonanruf gegenüber einem Verbraucher wirbt, hat dessen vorherige ausdrückliche Einwilligung in die Telefonwerbung zum Zeitpunkt der Erteilung in angemessener Form zu dokumentieren und gemäß Absatz 2 Satz 1 aufzubewahren.
(2) Die werbenden Unternehmen müssen den Nachweis nach Absatz 1 ab Erteilung der Einwilligung sowie nach jeder Verwendung der Einwilligung fünf Jahre aufbewahren. Die werbenden Unternehmen haben der nach § 20 Absatz 3 zuständigen Verwaltungsbehörde den Nachweis nach Absatz 1 auf Verlangen unverzüglich vorzulegen.“

Eine Missachtung kann übrigens zu einem Bußgeld von bis zu 300.000€ führen (UWG §20). Die Art der Einholung ist nicht vorgeschrieben, sicherste Methode ist wohl die Schriftform, gefolgt von der Gegenbestätigung (Double-Opt-In). Eine nachweislich, durchgehende Tonaufnahme kann es auch sein. Sicherheit wird – wie immer – erst eine höchstrichterliche Entscheidung bieten.

(n) BREXIT jetzt auch noch ex EU-Datenschutz?

09/2021 Bisher gilt für Großbritannien ein gleichwertiger EU - Datenschutz mit dem „Angemessenheitsbeschluss“ der EU – Kommission bis zum 27.06.2025 . Allerdings haben die Briten angekündigt, ihr Datenschutzrecht zu ändern (Haufe Online Redaktion 21.08.21)[115] und die

EU darauf mit einer Überprüfung. Eine Rücknahme der EU würden den Datentransfer mit GB verkomplizieren.

(o) E-Mail-Account gehackt! Was tun?

10/2021heise – online hat unter „E-Mail-Konto gehackt: Was Sie jetzt tun müssen“[116] einen hilfreichen Artikel veröffentlicht. Bei Unregelmäßigkeiten (wenig bis keine E-Mails, unbekannte Weiterleitungsregeln, Einstellungen oder Nachrichten im Papierkorb u. ä.) besteht der Verdacht auf einen Fremdzugriff. Was tun?: „Mit der notwendigen Ruhe sichern und zurückholen was möglich ist, Schwachpunkte erkennen und künftig vermeiden.

i) Keinerlei Zugriff mehr

Unbedingt mit dem E – Mail – Anbieter in Verbindung setzten (Online, Telefon, wie auch immer)

ii) Zugriff noch möglich

Alle Stecker ziehen und von einem sicheren Rechner auf das E-Mail-Account zugreifen und das Passwort ändern (mind. 10 Zeichen mit Großbuchstaben & Sonderzeichen) und angemeldete Geräte abmelden. Wenn möglich und im Angebot, a.) noch einen zweiten Faktor (SMS, Authenticator) hinzufügen und b.) separate Zugriffspasswörter für einzelne Anwendungen wählen (i. d. R. nur einmalig wieder anzumelden).

iii) Verknüpfungen prüfen

Wenn das E – Mail - Konto mit anderen Konten (Online – Banking, PayPal, Online – Shops, Amazon, ebay, Online – Spielplattformen, Cloud- und Streaming – Diensten, Social Media u.s.w.) verbunden ist, auf mögliche Schäden (unbekannte Bestellungen, Kontobewegungen u. ä.) prüfen und in jedem Fall auch hier das Passwort ändern.

iv) Sperren was notwendig ist, Anzeige erstatten

Über z. B. den SPERR-NOTRUF 116 116[117] können bei Verlust (girocard, Kreditkarten, Online – Banking, E – Personalausweis, SIM – Karten) von Daten, Karten oder Smartphones, diese sofort gesperrt werden. Wichtig ist ein Gespräch mit der Bank und die Anzeige bei der Polizei. Zum einen für eine Karten – SEPA – Lastschriftensperre[118] und zum Schutz vor Schäden aus Identitätsdiebstahl.

v) Spuren sammeln

Was ist in den E – Mails zu finden und könnte anderweitig genutzt werden (Name, Anschrift, Telefonnummer, Geburtsdatum, Zahlungsinformationen, fremde Kommunikation unter eigenem Namen, wichtige Dokumente). Vielleicht müssen auch Dritte, Freunde, Bekannte über einen möglichen Datenverlust und – missbrauch informiert werden.

vi) Schutzmaßnahmen

- Den befallenen Rechner professionell neu aufsetzen oder mit einem Rettungssystem[119] prüfen
- E – Mail – Adressen (über-) prüfen lassen, z. B. Firefox-Monitor[120] oder HPI Identy Leak Checker[11]
- Sichere Passwörter mit einem Passwortmanager erstellen und nutzen (z.B. Lockwise[121])
- 2 – Faktor – Sicherheit und separate Zugangsdaten für einzelne Software einrichten

(p) Whatsapp (Meta & Co) unverändert kritisch!

11/2021Unverändert bleibt der Einsatz von Whatsapp (Meta, Facebook & Co) im Datenschutz sehr kritisch! Und Firmen riskieren beim Messenger - Einsatz hohe Strafen (Welt)[122].

- ✗ Die beliebtesten Messenger – Dienst (bei Multihoming) nach einer Verbraucherumfrage der Bundesnetzagentur[123] sind Whatsapp 96%, Facebook 42%, Instegram 30% und Skype 18%.
- ✗ Nur eine Problemstellung: Adressbuchzugriff. So hat das AG Bad Hersfeld (AZ: F 120/17 EASO)[124] entschieden, dass es bei andauernder Datenweitergabe der Einholung einer Erlaubnis bedarf und für Kinder (<18 Jahren) Schutzvorkehrungen zu treffen sind und mehr …

(q) 11/2021Die TOP 5 der DS-GVO Bußgelder[125]

1.	746 Mio.€	Amazon Europe Core S.à.r.l	07/2021 „Werbung & Datenweitergabe“
2.	225 Mio.€	WhatsApp Ireland Ltd.	09/2021 „Informationspflichten & Datenweiterg.
3.	60 Mio.€	Google LLC	12/2020 „Tracking ohne Einwilligung“

4.	40 Mio.€	Google Ireland Ltd.	01/2021 „Tracking, fehlende DS-Hinweise“
5.	35 Mio.€	H&M	10/2020 „Mitarbeiterbespitzelung“
6.	27 Mio.€	TIM SpA	01/2020 „Werbeanrufe & Infomangel“

Nach Bericht der Landesbeauftragten für den Datenschutz NRW wurden im letzten Jahr in NRW 12.150 Beschwerden schriftlich eingereicht. Davon wurden insgesamt 631 Maßnahmen ergriffen (348 Hinweise, 23 Warnungen, 70 Verwarnungen, 54 Anweisungen, 1 Beschränkung, 123 Bußgeldverfahren eingeleitet und 93 Bußgeldbescheide erlassen).

(r) IT-Sicherheit & Datenschutz – kurzer Erklärungsversuch

12/2021

IT-Sicherheit ist der Schutz und die Abwehr von Gefahren und Risiken mit allen angemessen, zur Verfügung stehenden Mitteln.

Datenschutz oder Privatsphäre ist die Möglichkeit des Einzelnen, transparent und bewusst Risiken einzugehen, bzw. Daten freizugeben.

Datenschutz soll die Transparenz für eine bewusste und (rechtlich) sichere Entscheidung schaffen und die IT-Sicherheit keine technisch - anderweitige Verwendung gewährleisten.

(s) Smart Home & IoT: „INAKZEPTABEL“!

PDF-Link zur Ampelliste der Verkäufer

*12/2021*Begrifflich eingeschlossen sind auch WLAN – Router, Computer, wie vernetzte Business – Geräte und Medizintechnik. Heise online[126] berichtet aus einer Umfrage der IoT Security Foundation (seit 2018), dass 80% aller Vertriebsfirmen von IoT – Geräten gar nicht oder nur unzureichend auf gemeldete Sicherheitslücken reagieren, 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“ der Einordnung der Hersteller befindet sich auf Seite 20ff des Berichts der IoTSF[127].

(t) Sturz vom Bett zum Schreibtisch: Arbeitsunfall

*12/2021*Das Bundessozialgericht hat entschieden, ein Sturz im Homeoffice ist doch ein Arbeitsunfall. Die Handlungstendenz, hin zur beruflichen Tätigkeit entscheidet, es war ein Weg zur Arbeit. Wie t3n berichtet[128], hat ein Heimarbeiter seinen Treppensturz bei der Heimarbeit als Arbeitsunfall beantragt. Nach Ablehnung durch die Berufsgenossenschaft hat das Sozialgericht Aachen dafür, das Landessozialgericht Essen dagegen und das Bundessozialgericht Kassel zu guter Letzt für die Anerkennung entschieden.

(u) Operational Technology im Fadenkreuz[129]

*12/2021*Die Operational Technology oder Betriebstechnologie hat das Ziel für eine störungsfreie Produktion zu sorgen. Da oft Anlagenkomponenten mit eigener Steuerungssoftware & Wartung verschiedener Hersteller eingesetzt werden, ist alleine die Abstimmung des Sicherheitskonzeptes eine Herausforderung (Teilweise alte, nicht patchbare Betriebssysteme; mangelnde, integrierte Update - Funktion; unbekannte Kommunikationswege lt. Trend Micro[10]). Mit der fortschreitenden digitalen Transformation, hin zur Smart Factory, werden Webshop und ERP – System direkt mit der Produktion verbunden, was bisher getrennte Welten waren. Ein Überblick lohnt sich hier immer.

Bei Bedarf, einfach einmal sprechen!

Übersicht 2020 | Zum Datenschutz aufgefallen | Links aus der Fußnote

1 Quelle: BfDI: „Neue Homepage und Rückkehr Datenschutzforum“
2 Quelle: BfDI: „BDSG feiert 45jähriges Jubiläum“
3 Quelle: SDM – Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln" (PDF)
4 *NUR ZUR INFO* - BfA: SARS-CoV-2-Arbeitsschutzverordnung (Corona-ArbSchV) vom 20.01.2021
5 *Atemschutz in öffentlichen Bereich aktuell nur mit medizinische Masken (FFP2, OP-Masken) 01/2021*
6 Quelle: anwalt.de "Impfpflicht im Arbeitsverhältnis?"
7 Quelle: Coronavirus: die Fürsorgepflicht des Arbeitgebers – Mundschutz, Passierschein und Quarantäne
8 Quelle: DS-GVO Art.9 Abs.1, 2 / golem.de: „Merkel verteidigt Corona – App“
9 Quelle: SECURITYINSIDER „Datenschutz 2021“, & 10 IT-Security-Vorhersagen für 2021
10 Quelle: golem.de „WhatsApp stellt Nutzern ein Ultimatum“
11 Quelle: t3n Ratgeber: „WhatsApp – Alternativen“
12 Quelle: BfDI: „Nutzung von Messenger- und Videokonferenzdiensten in Zeiten der Corona-Pandemie“
13 Quelle: noyob: „Datenschutz bei Videokonferenzen“
14 Quelle: https://dejure.org/gesetze/DSGVO/Erwaegungsgruende.html siehe Punkt (82)
15 Quelle: https://dejure.org/gesetze/DSGVO/30.html
16 Quelle: https://dejure.org/gesetze/BDSG/70.html
17 Quelle: https://recht.nrw.de/lmi/owa/br_vbl_detail_text?anw_nr=6&vd_id=18927&sg=0
18 Quelle: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Corona
19 Quelle: LfDI Baden – Württemberg Info zu „DS-GVO.clever“ und direkt zum Tool „DS-GVO.clever“
20 Quelle: EU – Kommision / Recht / Datenschutz / Brexit
21 Quelle: https://www.duden.de/rechtschreibung/Anonymitaet
22 Quelle: https://dswiki.tu-ilmenau.de/pseudonymitaet
23 Quelle: https://dejure.org/gesetze/DSGVO/Erwaegungsgruende.html
24 Quelle: https://dejure.org/gesetze/DSGVO/4.html
25 Quelle: BfDI – Positionspapier – Anonymisierung unter der DS-GVO
26 Quelle: https://dejure.org/gesetze/DSGVO/9.html
27 Quelle: cloudcomputing – insider: „Deutsche Psychotherapeuten warnen vor der Cloud“
28 Quelle: https://volkerschroer.de/DSGVO/2021.01.31.InfoBrief.Datenschutz.Januar.pdf; Art.9 DS-GVO
29 Quelle: IfSG §8 „Zur Meldung verpflichtete Personen“
30 Quelle: DSK Pressemitteilung vom 29.03.2021 „Regelung Privatwirtschaft, Beschäftigungsverhältnisse“
31 Quelle: DSK Muss – Liste für den nicht öffentlichen Bereich
32 Quelle: anwalt.de: „Coronavirus: die Fürsorgepflicht des Arbeitgebers“
33 Quelle: Bundesregierung: „Corona-Warn-App Ver. 2.0 ermöglicht Eventregistrierung“
34 Quelle: PDF - Rückverfolgungsformular nach Infektionsschutzgesetz
35 Quelle: Welt-Online: „Corona-Tests für Arbeitnehmer können eben doch verpflichtend sein“
36 Quelle: Handelsblattartikel vom 13.04.2021; Prüfschema des BfDI zum Drittlandstransfer
37 Quelle: BfDI – „Prüfschema Drittlandstransfer“
38 Quelle: https://dejure.org/gesetze/DSGVO/49.html
39 Quelle: Entwurf unter FragDenStaat „Positionspapier der DSK bezüglich Microsoft Office 365“
40 Quelle: BSI „Konfigurationsempfehlung MS Office / 365“; MS Office /365 Rahmenempfehlung
41 Quelle: DS-GVO Art. 6; DS-GVO Erwägungsgründe (47)
42 Quelle: Microsoft: „Leitfaden für Datenverantwortliche, die Microsoft Office 365 verwenden“
43 Link: SZ: „Kleine Betriebe klagen über zu viel Bürokratie“ Tagesschau: „Zeitintensiver, mühsamer, teurer“
44 Link: https://volkerschroer.de/DSGVO/2021.04.15.Checkliste.Datentransfer.Drittland.pdf
45 Quelle: EDSA: „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von ...“
46 Link: „Zusammenfassung EDSA – Datentransfer Drittland zusaetzliche.Schutzmassnahmen“
47 Quelle: tagesschau.de: „Beschwerdewelle gegen Cookie – Banner“
48 Quelle: Zeit-Online: „Aktivist klagt vor Hamburger Landgericht gegen Onlinewerbung“
49 Quelle: iab Tech Lab: „Audiance Taxonomy“
50 Quelle: LDI – Hamburg: „Koordinierte Prüfung internationaler Datentransfers“
51 Quelle: EU Data Protection Supervisor: „Standardvertragsklauseln - SVK / SCC in diversen Sprachen“
52 Quelle: ntv „5 Mythen – Alle hassen den Datenschutz – zu Unrecht“
53 Quelle: Rundschreiben des BfDI und auf tagesschau.de, oder auf golem.de
54 Quelle: BfDI – Aufgaben und Befugnisse
55 Quelle: EuGH Nr. 81/18 vom 05.06.2018 Facebook-Fanpage & Art. 26 DS-GVO
56 Quelle: DSK – Orientierungshilfe „Schutzmaßnahmen bei E-Mail Übermittlung (Verschlüsselung)"
57 LINK: BSI TR-03108 "Sicherer E - Mail - Transport"
58 LINK: BSI TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“
59 LINK: §203 StGB „Verletzung von Privatgeheimnissen“
60 Quelle: HmbBfDI Verm. zur Abdingbarkeit von technisch-organisatorischen Maßnahmen (Art. 32 DSGVO)
61 Quelle: §79a Betriebsverfassungsgesetz
62 *Quelle*: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

63 Quelle: Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter in der EU / im EWR
64 Hinweis: Information zu „gemeinschaftlich Verantwortlich“ und Vertragsmuster
65 Hinweis: Muster Auftragsverarbeitungsvertrag nach Durchführungsbeschluss der EU – Kommission
66 Quelle: BMWi zum Gesetzgebungsverahren Netzpolitik (TTDSG)
67 Quelle der Urteile: Openjur.de: „OLG München 08.04.2010“ || Justiz.NRW.de: „AR Bonn 05.10.2016“ || juris.bundesgerichtshof.de: „BGH 01.02.2018“ || DSK – Online: „Orientierungshilfe Werbung 07.11.2018“
68 Quelle: DSK Entscheidung zur Impfstatusabfrage
69 Quelle: EuGH Nr. 81/18 vom 05.06.2018 Facebook-Fanpage & Art. 26 DS-GVO
70 Quelle: DSK Hinweise zum Verzeichnis von Verarbeitungstätigkeiten na Art.30 DS-GVO
71 Quelle: Dr. Datenschutz „Datenschutz bei Fotos: Wann findet die DSGVO Anwendung?“
72 Quelle: Projekt29: „Aktueller Fall aus einer Physiopraxis“
73 Quelle: Bundesamt für Justiz: „Infektionsschutzgesetz“
74 Quellen: GDD-Praxishilfe TTDSG (PDF) | Datenschutz-Guru | Datenschutz-Praxis;
75 Quelle: DSK: Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021
76 Quelle: TISiM: „Sec-O-Mat by TISiM - Ihr Weg zu mehr IT-Sicherheit“
77 Quelle: https://www.charteroftrust.com/about/
78 Quelle: Charter of Trust: „COVID 19 and how to securely work from home – key recommendations“
79 Quelle: heise online: „Exchange-Lücken: BSI ruft "IT-Bedrohungslage rot" aus“ & BSI – Info – Seite
80 Quelle: golem.de „LEAK“; t3n: „Vorsicht Telegram! ... Nutzer-/Chat-Inhalten lassen sich leicht abgreifen“
81 Quelle: FOCUS „1.000 Euro Schadensersatz? So bitten Sie Facebook im Datenskandal zur Kasse“
82 Link: BSI: SiSyPHuS Win10
83 Quelle: BMI – Kabinettsfassung zum „IT – SiG 2.0“; BMI: „Bundestag verabschiedet IT-Sicherheitsgesetz“
84 Quelle: Pojekt29: „Neue Studie der TU Darmstadt und IT-Seal GmbH zeigt: Social-Media-Nutzer sind“
85 Quelle: young date – open & safe: „Digitale Selbstverteidigung“
86 Quelle: bitkom: „Angriffsziel deutsche Wirschaft – Rekordschaden“
87 Quelle: Wikipedia: „Windows – Sysinternals“
88 Quelle: Microsoft-Docs: Process Explorer v16.43 / 18.08.2021 / Erläuterung & Download oder Liveausführung“
89 Quelle: Wikipedia: „VirusTotal.com“
90 Quelle: Mark Russinovich (Technischer Direktor Microsoft Azure) Video von der Tech Ed 2010“
91 Quelle: BSI Lagebericht 2021
92 Quelle: BSI: Awareness-Poster „Psychotricks und Phishing-Maschen“
93 Quelle: t3n „KI: Deepfakes sind eine Gefahr für die Demokratie – sagt eine EU-Studie“
94 Quellen: Spektrum.de: „Offen für alles“; BayLfD: „Handreichung & Erstanalyse“; heise-online: Schutz … was hilft …“
95 Quelle: BSI: „Awareness - Poster“
96 Quelle: Tagesschau.de: „Fraglicher Datenschutz im Clubhouse“; „ICON: „Cubhaus?“
97 Quelle: Handelsblatt: „Verbraucherschützer mahnen Betreiber von Clubhouse-App ab.“
98 Quelle: Süddeutsche Zeitung: „Der Ransomware-Schrecken des deutschen Mittelstands“
99 Quelle: Link zur Pressemitteilung des BfDI
100 Quelle: Link Pressemitteilung BMWi | Link BMWi Gesetzentwurf TTDSG | Link TTDSG-Entwurf BMWi
101 Quelle: Der Tagesspiegel „Wenn Datenschutz zur Ausrede wird“
102 Quelle: BSI „IT – Grundschutzkompendium – Werkzeug für die Informationssicherheit“
103 Quelle: heise online "Microsoft verspricht weniger Überwachung Einzelner in Microsoft 365"
104 Quelle: Frankfurter Zeitung „Am Rhein brennt Europas Datenschatz“ | CloudComputing-Insider
105 Quelle: Süddeutsche Zeitung „Schufa will Konten der Deutschen durchstöbern“
106 Quelle: Südeutsche Zeitung "Schufa stampft umstrittenes Projekt ein"
107 Quelle: https://nordvpn.com/de/national-privacy-test/ und der Ländervergleich als PDF
108 Quelle: BKA Bundeslagebild Cybercrime 2020
109 Quelle: https://bigbrotherawards.de/2021 & t3n: „Doctolib hat Suchanfrage mit …..“
110 Quelle: Finance „Diese 4 Betrugsmaschen …“ DerTreasurer „… umgekehrte Scheckbetrug ...“
111 Quelle: Euler-Hermes – „ … erster Fall ... KI-Software“ | Der Treasurer „Erste Schritte nach Angriff“
112 Quelle: heise-online: „Das Conti-Leak: Bedienungsanleitung für Ransomware“
113 Quelle: Deutscher Bundestag: Gesetzentwurf „für faire Verbraucherverträge“ (19/26915)
114 Quelle: Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 53 Punkt 7, ausgegeben zu Bonn am 17. August 2021
115 Quelle: haufe online redation: „Großbritannien will Datenschutz reformieren und sich von der DSGVO lösen“
116 Quelle: heise-online: „E-Mail-Konto gehackt: Was Sie jetzt tun müssen“
117 Quelle: Sperr-Notruf 116116: https://www.sperr-notruf.de/
118 Quelle: KUNO: Karten-Sperrdients für SEPA – Lastschriftzahlungen (nur Unterschrift)

119 Quelle: Beispiel für ein Rettungsystem: Desinfec’t von heise – Online (Artikel)
120 Link: https://support.mozilla.org/de/kb/firefox-monitor; https://sec.hpi.de/ilc/
121 Link: https://www.mozilla.org/de/firefox/lockwise/
122 Quelle: Welt: „Firmen riskieren beim Messenger-Einsatz hohe Strafen“
123 Quelle: Bundesnetzagentur: „Bundesnetzagentur veröffentlicht Bericht zu Online-Kommunikationsdiensten“
124 Quelle: AG Bad Hersfeld: „AZ: F 120/17 EASO“
125 Quelle: GDPR Enforcement Tracker; DSGVO – Portal – Geldbußen; zu NRW LfDI – NRW - Bericht
126 Quelle: heise online: Sicherheitslücken bei Smart Home & IoT: Hersteller arbeiten „inakzeptabel“
127 Quelle: IoTSF: The Contemporary Use of Vulnerability Disclosure in IoT Report4. November 2021
128 Quelle: t3n: „Urteil gefällt: Sturz im Homeoffice ist doch ein Arbeitunfall“
129 Quelle: Telekom: „OT im Fadenkreuz“; Trend Micro: „Schützen Sie Ihre IoT-Geräte in OT-Systemen“