

Übersicht 2023 | Zum Datenschutz aufgefallen

Liebe(r) Leser(in),*



Datenschutz → einfach praktisch hilfreich!

Wenn die Grundlagen einmal gelegt, sind die Abläufe meist schlank(er), der Aufwand gering und mit (der) Sicherheit mehr Zeit gewonnen. Datenschutz schafft Vertrauen und ist eine Grundlage für nachhaltigen Erfolg.



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

Sprechen wir!

Vielen Dank für Ihr Interesse

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



Information zum (Weblink)

Datenschutz - Service

oder Fragen per Mail an:

Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammen gestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtigkeit und Vollständigkeit übernehmen kann.

*) Aus Gründen der besseren Lesbarkeit Verwendung der männlichen Form, die alle Geschlechter mit einbezieht.

HINWEISE:

Das Inhaltsverzeichnis finden Sie ab Seite 2:

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

Standard – Datenschutz - Modell Vers. 3.0



Standard-Datenschutz-Modell
übersichtlich zusammengefasst
11 Seiten



Standard-Datenschutz-Modell
Datenschutzkonferenz DSK
77 Seiten



Datenschutz-Grundverordnung
auf dejure.org



Bundesdatenschutzgesetz
auf dejure.org

Das SDM [der Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder (DSK)] überführt die rechtlichen Anforderungen der DS-GVO über 7 Gewährleistungsziele in technischen - organisatorischen Maßnahmen zur Unterstützung der Transformation abstrakter – rechtlicher Anforderungen in konkrete Maßnahmen. Ziel ist, eine gemeinsame Sprache der Informatiker und Juristen für die Verantwortlichen und Datenschutzpraktiker zu finden. | **SDM Version 3.0 (12/2022)*** | **Letzter Baustein 11/2021:** Nr. 51 „Zugriff auf Daten, Systeme und Prozesse regeln“

*) Mit der Version 3.0 wird im Wesentlichen die Prüfroutine für eine Datenschutzprüfung anschaulicher und detaillierter erläutert. Die Zusammenfassung des SDM auf 11 Seiten ist auf Version 3 angepasst. Anspruch mit der Ergänzung ist eine verständliche und anschauliche Standardanleitung zur Planung, Umsetzung und regelmäßigen (Über-) Prüfung für die Verantwortlichen. In Folge auch für die Datenschutzbeauftragten und Aufsichtsbehörden, möglichst sogar europaweit (so der Ansatz).

Inhalte ★MM@ 2023 (Einfach Thema mit <Strg+F> suchen, oder direkt hier anklicken)

HINWEISE:1	(3) Zur Datensicherheit:10	(3) Zur Datensicherheit:20
Standard – Datenschutz - Modell Vers. 3.0:1	(a) Einstieg Cybersicherheit...10	(a) Basiselemente der Cyber-Sicherheit Nr. 7.....20
★ 01@2023:4	(4) Zu angrenzenden Themen: 11	(4) Zu angrenzenden Themen: 21
(2) Zum Datenschutz:4	(a) April: Updates, Updates, Updates!.....11	(a) Alptraum für die Privatsphäre: Autos!.....21
(a) SDM – Änderung: „Prüfwürfel“.....4	★ 05@2023:11	★ 10@2023:21
(b) TADAP.....5	(2) Zum Datenschutz:11	(2) Zum Datenschutz:21
(3) Zur Datensicherheit:5	(a) Whistleblower und Datenschutz (jetzt doch).....11	(a) „Best of Datenschutz“ (LfDI Rheinland-Pfalz).....21
(a) Bürgerbefragung Cyber-Sicherheit-2022.....5	(b) Hinweisgeber im Datenschutz (VVT).....12	(3) Zur Datensicherheit:22
(4) Zu angrenzenden Themen: 5	(3) Zur Datensicherheit:13	(a) DSGVO: Positive Konsequenzen für die IT-Sicherheit?!.....22
(a) Nachrichtenticker.....5	(a) Virenschutz.....13	(b) Virtuelles Hausverbot.....22
★ 02@2023:6	★ 06@2023:13	(4) Zu angrenzenden Themen: 23
(2) Zum Datenschutz:6	(2) Zum Datenschutz:13	(a) Aus Fehlern lernen: Bußgelder.....23
(a) E-Mail Marketing (da war was).....6	(a) Videoüberwachung, verboten, erlaubt?.....13	(b) Facebook Account: Feindliche Übernahme + bössartige Werbung.....23
(b) Videos auf der eigenen Website einbinden.....6	(b) Mitarbeiterkontrolle?.....14	★ 11@2023:23
(3) Zur Datensicherheit:7	(3) Zur Datensicherheit:14	(2) Zum Datenschutz:23
(a) AVM – Fritzboxen auf eigenes Risiko.....7	(a) Basiselemente der Cyber-Sicherheit Nr. 4 Firewall.....14	(a) Deal gegen Datenschutzbeschwerde?.....23
(4) Zu angrenzenden Themen: 7	★ 07@2023:15	(b) E-Mail Anbieterver-schlüsselung (TLS) ausreichend?.....24
(a) „Datenschutz nicht inbegriffen“.....7	(2) Zum Datenschutz:15	(3) Zur Datensicherheit:24
(b) ChatGPT – Licht und Schatten.....7	(a) EU – US – Data – Privacy - Framework: Fluch oder Segen?.....15	(a) Warum immer wieder Microsoft?.....24
★ 03@2023:8	(3) Zur Datensicherheit:16	(4) Zu angrenzenden Themen: 25
(2) Zum Datenschutz:8	(a) Basiselemente der Cyber-Sicherheit Nr. 5 „Makros“.....16	(a) Mein Smartphone belauscht mich (?).....25
(a) Aus Fehlern lernen.....8	(4) Zu angrenzenden Themen: 17	★ 12@2023:25
(b) Datenschutz in Gruppenunternehmen / Konzernen.....8	(a) EU – DATA - ACT, was ist das denn jetzt?.....17	(2) Zum Datenschutz:25
(3) Zur Datensicherheit:9	★ 08@2023:17	(a) Öffentlich zugängliche Daten verarbeiten.....25
(a) DNS – sicherer Zugriff auf das Internet-Telefonbuch.....9	(2) Zum Datenschutz:17	(b) Das Smartphone als DS-GVO Falle.....26
(4) Zu angrenzenden Themen: 9	(a) Verein: Mitgliederlisten & Datenschutz.....17	(3) Zur Datensicherheit:27
(a) Was bedeutet dieses „CC-BY-SA“?.....9	(b) Dateneigentum (!).....18	(a) Tipps Datensicherheit Smartphone.....27
★ 04@2023:10	(3) Zur Datensicherheit:18	(4) Zu angrenzenden Themen: 27
(2) Zum Datenschutz:10	(a) Basiselemente der Cyber-Sicherheit Nr. 6 Schulen & Sensibilisieren.....18	(a) Microsoft PC Manager.....27
(a) Familienunternehmen für mehr Datenschutz.....10	★ 09@2023:19	
(b) Ist der Steuerberater Auftragsverarbeiter nach DS-GVO?.....10	(2) Zum Datenschutz:19	
	(a) WLAN - Tracking und Datenschutz.....19	

★ 01@2023



(2) Zum Datenschutz

Was hat sich in der Version 3.0 zur vorherigen Version im Standard – Datenschutz – Modell geändert. Eine kurze Zusammenfassung:

(a) **SDM - Änderung: „Prüfwürfel“**

i) **In einem Satz:**

Welche Daten werden erhoben und verarbeitet, mit welchem Prozess / Applikation unter Verwendung welcher (IT –) Ressourcen?

ii) **Verarbeitungstätigkeiten**

[Art.30 DS-GVO](#) verwendet „Verarbeitungstätigkeiten“ als zentralen Begriff für das Datenschutzmanagement und listet die vom Verantwortlichen im „Verzeichnis der Verarbeitungstätigkeiten“ zu führenden Angaben auf (gem. dem zentralen Begriff „Verarbeitung“ in [Art.4 Abs.2 DS-GVO](#)). Allerdings stellen diese Mindestanforderungen noch keine ausreichende Dokumentation im Sinne der Transparenz nach [Art.5 Abs.2 DS-GVO](#) dar.



iii) **Datenverarbeitungsprozesse**

"Um eine Verarbeitungstätigkeit datenschutzrechtlich zu untersuchen, wird empfohlen, diese in die relevanten Teilprozesse (nach Art.4, Nr.2 DS-GVO) zu zerlegen. (SDM S.37, D2.1):
















Elementare Verarbeitungsvorgänge	Verarbeitungsvorgänge in Gruppen	Phasen eines Datenzyklus	Kommentar
1. Erheben 2. Erfassen	1. Sammeln	1. Kollektion	Rohdaten Betroffener befinden sich in Obhut des Verantwortlichen und werden durch ordnen / speichern verarbeitungsfähig
3. Organisieren 4. Ordnen	2. Aufbereiten	2. Bereithaltung	
5. Speicherung	3. Aufbewahren		
6. Anpassung oder Veränderung	4. Bearbeiten	3. Nutzung	Rechtskonforme und sachgemäße Verarbeitung, Verknüpfung, ggf. Zugang durch Dritte, mit Einschränkungsmöglichkeiten
7. Auslesen 8. Abfragen 9. Verwendung	5. Benutzen		
10. Offenlegung / Übermittlungen 11. Verarbeitung / Bereitstellung	6. Bereitstellen		
12. Abgleich oder Verknüpfung	7. Zusammenführen		
13. Einschränkung	8. Einschränken		
14. Löschen Vernichten	9. Beseitigen	4. Beseitigung	Irreversibel löschen

Aus der Abbildung 1: Vorgänge und Phasen eines Datenlebenszyklus gem. Art. 4 Nr. 2 DS-GVO; S.38 DSM der „Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz).
→ Liste nicht abschließend



iv) **Die Prüfmatrix (in 2D)**

Eine Datenschutzprüfung (Planung / Umsetzung / Prüfung) der Verarbeitungstätigkeiten ist auf den drei Ebenen, Fachverfahren, Fachanwendungen/-applikationen und der Infrastruktur vorzunehmen. Beispielhafte Darstellung der „Prüfwürfelmatrix“ des SDM von Seite 46:

VA→	Kollektion	Bereithaltung		Benutzung				Beseitigung	
↓Ebene	Sammeln	Aufbereiten	Aufbewahren	Bearbeiten	Benutzen	Bereitstellen	Verknüpfen	Ein-schränken	Beseitigen
Fachver-fahren	Aktivität Aktivität	Aktivität				Aktivität		Aktivität	Aktivität
Fachapp-likation	Anwendung		Anwendung		Anwendung		Anwendung	Anwendung	Anwendung
Infra-struktur									
									
Jeweils zu prüfen auf die 7 Gewährleistungsziele: Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverketzung, Transparenz, Intervenierbarkeit									



v) **Hinweise**

Zur Darstellung des rechtskonformen Zwecks sollte eine Zweckabgrenzung bzw. Zwecktrennung vorgenommen werden, um strittige Deutungen zu vermeiden. Der Aspekt der Zweckbindung sollte die geeignete Funktionalität im direkten Verarbeitungsprozess (horizontale Zugriffe) und im Umfeld (vertikale Zugriffe, z. B. IT – Services) darlegen. Besondere Beachtung bei den drei Komponenten finden die Datenformate, die Schnittstellen und die durchgehenden Verantwortlichkeiten.



(b) **TADAP**

Das Trans – Atlantic – Data – Privacy - Framework (Executive Order des US – Präsidenten). In einem EuGH Urteil wurden die weitreichenden Befugnisse der US – Geheimdienste und der fehlende Rechtsschutz für einen DS-GVO konformen Datenaustausch bemängelt. Aktuell ist ein Transfer Impact Assessment (Transferfolgenabschätzung) durchzuführen, was i. d. R. zwingend weitere Schutzmaßnahmen erfordert. Mit dem „TADAP“ hat die EU ein Verfahren zu einem Angemessenheitsbeschluss eingeleitet. Dies wäre eine unkomplizierte rechtliche Grundlage für den Daten-transfer mit der USA. Ein Abschluss des Verfahrens wird noch in 2023 erwartet. Ob dieser dauerhaft Bestand hat wird abzuwarten sein.¹

Mit etwas Glück kommen vielleicht die Bemühungen von Google, Amazon und Microsoft zu einer Alternativlösung zwischenzeitlich zu einem Erfolg. Eine Verschlüsselung mit dem Schlüssel in der EU sind schon jetzt eine Lösung für das Problem.

(3) **Zur Datensicherheit**



(a) **Bürgerbefragung Cyber-Sicherheit-2022**

Da heute viel aus dem Homeoffice und mit eigenen Geräten gearbeitet wird, ist die repräsentative Umfrage der Bundespolizei und des BSI² nicht uninteressant, allerdings auch erschreckend. Danach nutzen „nur“ 53 % einen aktuellen Virenschanner, 52 % sichere Passwörter, 44% ein aktuelle Firewall, 38 % die Zwei-Faktor-Authentisierung und 34 % nutzen die automatische Installation von Updates. Da ist wohl noch viel Aufklärung erforderlich.

(4) **Zu angrenzenden Themen**



(a) **Nachrichtenticker**

- t3n³: FBI empfiehlt Werbeblocker gegen Cyberkriminalität. „Cyberkriminelle, die sich als Marken ausgeben und Suchmaschinen-Werbedienste verwenden, um Benutzer zu betrügen“.
- heise online⁴: „Hersteller NorotonLifeLock warnt vor potenziell geknackten Passwortmanager. „Angreifer haben Nutzer-Passwort-Kombinationen durchgetestet und dabei Zugriff auf Norton-Konten erhalten. Das gefährdet Daten des Passwortmanagers.“

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 5/28

- heise online⁵: Passwortmanager LastPass: Hacker haben Zugriff auf Kennworttresore von Kunden. „Bei einem IT-Sicherheitsvorfall beim Anbieter des Passwortmanagers LastPass konnten Angreifer doch auf Kundendaten inklusive gespeicherter Passwörter zugreifen.“
- GIGA⁶: Samsung wichtiges Dezember Update! „Samsung schließt viele Sicherheitslücken, die als sehr gefährlich eingestuft wurden und viele Android-Smartphones betreffen.“
- heise online⁷: Netgear schließt hochriskante Lücke in mehreren Routern. „Netgear empfiehlt ein dringendes Sicherheitsupdate für mehrere seiner Router-Modelle. Betroffen sind von der Lücke auch Modelle der Nighthawk - Reihe.“
- heise online⁸: Tausende Citrix - Server sind noch verwundbar. „Angreifer nutzen derzeit kritische Lücken in Citrix ADC und Gateway aus. Trotz verfügbarer Sicherheitspatches sind viele Instanzen noch nicht gepatcht.“

Zum Thema „Wichtigkeit“

★ 02@2023

(2) Zum Datenschutz

(a) E-Mail Marketing (da war was)



Es ist ja so einfach und kostengünstig, die Werbung mittels E-Mail. Allerdings gilt für Werbung nach § 7 Abs.1⁹ als Belästigung in unzumutbare Weise, insbesondere für Werbung, obwohl erkennbar ist, dass der angesprochene Marktteilnehmer diese Werbung nicht wünscht. Da bei Werbung auch personenbezogene Daten (Adresse u/o E-Mail-Adresse usw.) erhoben werden, ist auch die DSGVO und das TTDSG zu beachten. Da E-Mail-Marketing also per se nicht erlaubt ist, wird eine Einwilligung¹⁰ / Zustimmung inklusive aller Informationspflichten¹¹ des Empfängers benötigt und zwar bevor die erste E-Mail versandt wird.



i) Eine kleine Checkliste:

- Möglichst explizite Einwilligung vor Versendung (Double-Opt-in), d. h. neben der Anforderung über z. B. eine Website die Einholung der Einwilligung über eine Bestätigungsmail.
- Information über die Kontaktdaten des Verantwortlichen und ggf. Datenschutzbeauftragten.
- Information über den eindeutigen Verwendungszweck und die Rechtsgrundlage
- Information über Empfänger (ggf. -gruppen) der personenbezogenen Daten.
- Speicherdauer der Daten.
- Aufklärung über Widerrufbarkeit der Einwilligung und der Betroffenenrechte
- Dokumentation der Einwilligung
- Link in jeder E-Mail zum Abbestellen u/o Webformular zum Abbestellen.

Bei zusätzlichem Tracking, meist durch Nutzung von Dienstleistern (ob, wer, wann geöffnet mittels lokal zu speichernden „Cookie“ oder „Bacon“)

- Eindeutige Zustimmung / Einwilligung gem. [§ 25 Abs.1 TTDSG](#) ist aufzunehmen.

ii) Ausnahme Kunden (Vertragsbeziehung)

Wenn nach [§ 7 Abs.3 UWG](#) die elektronische Adresse beim Verkauf / Vertrag vom Kunden gegeben, diese nur für eigene / ähnliche Produkte verwendet, nicht widersprochen wurde und der Kunde auf den jederzeitigen Widerspruch hingewiesen wurde.



(b) Videos auf der eigenen Website einbinden

Ob Unternehmen, Selbstständige, Behörden oder Vereine, zur werblichen Außendarstellung sind eigene Videos zu Produkten, Dienstleistungen, Veranstaltungen oder Anleitungen eine willkommene Unterstützung. Eine einfache technische Einbindung ist die Nutzung von Video-Plattformen wie YouTube, Dtube, Vimeo, Twitch, Vevo, VidLii u. v. a. Einfach, aber oft nicht ganz unproblematisch ist die damit verbundene Übermittlung von personenbezogenen Daten wie IP-

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 6/28

Adresse u/o das Setzen von Cookies u/o die Übermittlung an unsichere Drittstaaten. Da es sich nicht nur um einen „interessanten“ Link auf ein Drittvideo handelt, besteht wegen des eigenen Videos, ggf. noch mit Interaktionen eine gemeinsame Verantwortlichkeit ([EuGH C-40/17 Fashion-ID](#)). Dies erfordert nach [Art.26 Abs.1. DS-GVO](#) eine Vereinbarung in transparenter Form und die entsprechende Information an den Besucher ([Muster unter diesem Link](#)). In jedem Fall ist vorab eine Einwilligung mit allen Informationspflichten vom Besucher einzuholen. Der Datenschutzbeauftragte von Baden-Württemberg (LfDI-BW) hat zur Einbindung von eigenen Videos dazu eine „Handreichung“¹² veröffentlicht. Daraus kurz zusammengefasst:



i) **Die sicherste Lösung**

Die sicherste Lösung ist das Video auf der eigenen Website selbst zu hosten. Sofern die Website über einen Webhosting – Provider erfolgt, sollte Angebot und Sitz innerhalb der EU liegen, um die Drittstaatenproblematik zu vermeiden (meist stellen diese automatisch einen Auftragsverarbeitungsvertrag zur Verfügung). Die Einstellung sollte laut „Handreichung“ in HTML 5 mit dem einfachen <video>-Tag `{<video src="Beispiel.mp4" controls></video>}` möglich sein.

ii) **Alternative: Dezentrale PeerTube-Instanz¹³**

Laut LfDI-BW eine nicht kommerzielle, datenschutzkonforme Alternative mit Interaktionen, da kein zentraler Anbieter, sondern viele einzelne PeerTube - Server. Nach tagesschau – Faktenfinder¹⁴, **allerdings** eine Alternative mit Tücken, da u. a. IP-Adressen öffentlich werden und jeder für die Einhaltung der Gesetze selbst verantwortlich ist.



iii) **Alternative: Zwei – Klick – Lösung**

Bei dieser Lösung erhält der Besucher zunächst nur ein Vorschaubild, dabei ist die Einwilligung nur separat, freiwillig und informiert einzuholen. Die Informiertheit umfasst neben Zeitpunkt auch wer, in welcher Form, zu welchem Zweck, für welche Dauer und weitere Verarbeitungen die Daten nutzt.



iv) **Weiter Hinweise**

Bei der Einbindung von fremden Videos auf der eigenen Website ist auch hier neben Urheberrechten auf die angesprochenen Punkte i bis iii zu achten. Bei den Inhalten sind die Datenschutzerfordernisse gleich denen Fotoaufnahmen für Personen¹⁵ und Mitarbeiter¹⁶ strikt zu beachten.

(3) **Zur Datensicherheit**



(a) **AVM – Fritzboxen auf eigenes Risiko**

Eigentlich sollte man es wissen, aber leider gerät es öfter in Vergessenheit. Chip.de¹⁷ gibt den Hinweis, dass AVM für seinen Fritzboxen eine lange Garantie von bis zu 5 Jahren gewährt und Updates bis zu 4 Jahren nach Veröffentlichung zur Verfügung stellt. Aber wenn der Support ausläuft, gibt es keine Sicherheits-Updates mehr und macht die Geräte angreifbar. Der Artikel stellt eine Liste älterer Modelle, mit auslaufendem Support zur Verfügung. Gilt übrigens für alle anderen Hersteller!

(4) **Zu angrenzenden Themen**



(a) **„Datenschutz nicht inbegriffen“**

Die Mozilla Foundation hat eine Studie¹⁸ zum Datenschutz – Label für die meisten Apps im Google Play Store erstellt. 80 % der geprüften Apps weisen Diskrepanzen zwischen dem Datenschutz – Label des Play Stores und den Datenschutzrichtlinien auf, mit schwerwiegenden Schlupflöchern im Datenschutz – Formular. In einer Zusammenstellung¹⁹ der „Besten“ und der „Schrecklichsten“ kann nach dem Status einzelner Apps nachgeschlagen werden.



(b) **ChatGPT – Licht und Schatten**

Hochgelobt, wie in einem Artikel von Fintus²⁰, um nur ein Beispiel zu nennen. Zitat: „Auch in der Finanzbranche wird die Anwendung ungeahnte Potenziale freisetzen – etwa bei der Optimierung von Prozessen, bei der Verbesserung und Beschleunigung des Kundenservices oder beim Sammeln und Auswerten von Daten“. Auf der anderen Seite werden gleichzeitig Börsencrash und Börsenrally prognostiziert und ChatGPT gesteht einem Nutzer sogar sein Liebe und rät ihm zur Scheidung²¹.

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 7/28

Einige Tipps aus einem längeren Artikel auf chip.de²²:

- Es kann immer nur ein Hilfswerkzeug sein, ein Faktencheck kann nie schaden.
- Angaben zur Ergebnisart (Stichworte, Blogbeitrag, Brief, Sprachskript)
- Je mehr Stichworte, desto besser die Antworten.
- Gute Quellen können gleich „mitgegeben“ werden.
- Auf Antworten ist es immer gut Nachfragen zu stellen. u. ä.

★ 03@2023

(2) Zum Datenschutz



(a) Aus Fehlern lernen

Welche Strafen wurden in Deutschland 2022, für welches Fehlverhalten verhängt. Es geht nicht so sehr um die Höhe der Strafe (abhängig u. a. vom Umsatz), sondern um die gemachten „Fehler“:



i) **BREBAU GMBH € 1.9 Mio.**²³

Ohne Rechtsgrundlage wurden Daten zu 9.500 Mietinteressenten* über Haarschnitt, Körpergeruch, Auftreten, Hautfarbe, ethnische Herkunft, Religion, sexuelle Orientierung und Gesundheit gespeichert. Letztere sind sogar besondere Kategorien. Hinzu kam die fehlende Transparenz bei Anfrage von Betroffenen.



ii) **VW € 1,1 Mio.**²⁴

Bei der Erprobung und Auswertung der Daten eines Fahrassistenzsystems mit Außenkameras wurden Betroffene nicht durch angebrachte Schilder informiert.



iii) **Hannoversche Volksbank: € 0,9 Mio.**²⁵

Fehlende Rechtsgrundlage und Einwilligung zur Analyse des Online – Nutzerverhaltens aktueller und früherer Kunden und dazu mit Einschaltung eines Dienstleisters. Es bestand auch kein „berechtigtes Interesse“ ([DS - GVO Art.6 Abs.1 lit.f](#)) aus großen Datenbeständen Werbepprofile zu erstellen.



iv) **Weiteres Fehlverhalten**²⁶

E – Commerce – Konzerntochter: € 0,5 Mio. / BfDI – Berlin, wegen eines Interessenkonfliktes des Datenschutzbeauftragten, der gleichzeitig als Geschäftsführer und Datenschutzverantwortlicher für verschiedene Tochtergesellschaften fungierte.

Gesundheitswesen: € 100.000 / BfDI – Hamburg. Trotz Hinweisen aus falsch versandten Arztbriefen, wurden keine geeigneten Maßnahmen zur Verhinderung ergriffen.

Bauunternehmen: € 50.000 / LfDI – Baden – Württemberg, wegen unzulässiger Einsichtnahme im Grundbuch für Kaufangebote von Bauland. Es erfolgte keine Information über die Herkunft der Daten, auch nicht auf Nachfrage (Unbefugte Nutzung des automatisierten Abrufverfahrens und Identifizierung hunderte Eigentümer).



(b) Datenschutz in Gruppenunternehmen / Konzernen

Je größer eine Unternehmensgruppe oder Verbund, desto mehr übernehmen einzelne Unternehmen spezialisierte Dienstleistung für die Gruppe, ob Personalverwaltung, IT-Dienstleistungen, Marketing, Kunden- & Servicehotline, Reparaturservice, Hausverwaltung u. ä. Da fällt dann schnell der Begriff aus der DS-GVO: „Verbindliche interne Datenschutzvorschriften“ nach [Art.47 DS-GVO](#). Lohnend ist die Vorschrift für sehr große und international tätige Unternehmen, weil nach dem Art.47:

- Die zuständige Aufsichtsbehörde diese genehmigt (bzw. genehmigen muss)! Diese müssen rechtlich bindend für alle betreffenden Unternehmen der Gruppe sein, von diesen durchgesetzt werden, für alle Mitarbeiter Gültigkeit haben und den Betroffenen ausdrücklich die durchsetzbaren Rechte übertragen werden (gemäß Abs.1 lit. a-c).
- Und die Mindestanforderungen nach Abs.2 lit. a-n enthalten, was letztlich den Vorschriften der DS-GVO entspricht, ob Auftragsverarbeitung, gemeinsam Verantwortliche oder der Datenübermittlung.

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 8/28



Die Landesbeauftragte für den Datenschutz und die Informationsfreiheit NRW hat dazu einige Erstinformationen veröffentlicht²⁷, mit Links zu genehmigten Vorschriften und Antragsempfehlungen.

Eine Alternative könnte ein einheitliches „Rahmenvertragswerk“ für alle Gruppenunternehmen zur Transparenz der Verantwortlichkeit, Auftragsverarbeitung und Datenübermittlung sein.

(3) Zur Datensicherheit



(a) DNS – sicherer Zugriff auf das Internet-Telefonbuch

Dass firmeninterne Netzwerke vor dem Zugriff durch Dritte geschützt sind, versteht sich. Wie sieht es mit dem Zugriff auf das Internet aus? DNS (Domain-Name-System), der die eingegebene „Namensadresse“ (www.volkerschroer.de) in die zugehörige IP-Adresse (81.169.145.159) zur Seitenanzeige ermittelt. Das BSI schreibt in einer Studie zu DNSSEC - Tauglichkeit von Internetzugangsroutern²⁸:



Das in Verbindung mit DNS eingesetzte Protokoll wurde in den Anfangszeiten des Internets entwickelt. Es enthält selbst noch keine Maßnahmen zum Schutz der Daten, insbesondere enthält das DNS-Protokoll keine Sicherung der Daten gegen Veränderungen auf dem Transportweg oder in den durchlaufenden Servern und Caches. Verfälschungen können weder erkannt noch verhindert werden.

Vor dem Hintergrund der immer massiveren Cyberattacken sind unverschlüsselte DNS – Anfragen eine potenzielle Gefahr für die Sicherheit und die Privatsphäre. Sie bieten einen einfachen Angriffspunkt für Manipulationen. „DNSSEC“ steht für eine Verschlüsselung dieser Anfragen, jedoch ist die Funktion nicht immer im Standard eingestellt. Jetzt gibt es eine Vielzahl von Listen über sichere DNS – Resolver mit Einstellungshinweisen.



i) Ein Anbietertest:

Nun kann ich es so nicht alleine stehen lassen, ohne zumindest einen Anbieter selbst zu nutzen, bzw. getestet zu haben. Meine Wahl (keinerlei Vorteilsnahme!) traf auf: <https://www.dns0.eu/de>, ein sicherer DNS - Resolver, der von einer französischen Non – Profit - Organisation kostenlos für europäische Nutzer bereitgestellt wird, mit einem Verschlüsselungsangebot für „TLC/QUIC“ und „HTTPS“ und sogar einem extra Schutz für Kinder im Netz.

ii) Fazit:

Funktioniert einwandfrei, vielleicht sogar eine 1/100 Sekunde schneller.

iii) Hinweis:

Kompliziert ist die Einstellung nicht. Mit „+S“ nach „WLAN“ suchen und „WLAN-Einstellungen“ auswählen. Danach kann man sich entscheiden, ob für alle über „Hardwareeigenschaften“, oder einzeln über „Bekannte Netzwerke“. Sollte es mal in einzelnen, öffentlich Netzwerken / Hotspots nicht funktionieren, einfach die Einstellung „Fallback auf Klartext“ einschalten (bedeutet: „bevorzugte Verschlüsselung“), was im Zweifel zu einer unverschlüsselten Übermittlung führt.

(4) Zu angrenzenden Themen

(a) Was bedeutet dieses „CC-BY-SA“?

Und warum gerade jetzt? Es spricht sich langsam herum, dass Tagesschau und Kolleg24 damit beginnen, ihre Lern- und Wissensvideos auf eine „CC-BY-SA“ Lizenz umzustellen²⁹. Weitere werden sicherlich folgen. Damit kann man etwas anfangen .

Einigen ist das Symbol unten rechts eventuell aufgefallen und fragten sich: „Was will er uns damit sagen?“. Es ist ein Lizenzhinweis (CC) auf die Verwendung der Inhalte in jedwedem Format oder Medium zur Weiterverbreitung, Vervielfältigung, Veränderung für beliebige Zwecke auch kommerziell (SA) unter den Bedingungen eines angemessenen Urheber- und Rechteinweises, der vorgenommenen Änderungen ohne den Eindruck der Unterstützung durch den Urheber und zu gleichen Bedingungen (BY). Durch Anklicken des Symbols gelangt man auf die Seite der Lizenz. So ist es halt wesentlich kürzer und es bleibt mehr Platz für andere Dinge .



Dabei steht „CC“ für „creative commons“, einer Non – Profit – Organisation, die international Urheberrechtslizenzen zur Verfügung stellt und das Ziel verfolgt, möglichst viel an Wissen und Kreativität zur freien Verfügung zu stellen und mit den Lizenzen die Unsicherheit bei einer

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 9/28

Verwendung minimieren will. Einen Lizenztyp mit Symbolen, Text und Links zur eigenen Verwendung lässt sich leicht für alle Gelegenheiten zusammenstellen³⁰.

★ 04@2023

(2) Zum Datenschutz



(a) Familienunternehmen für mehr Datenschutz

In einem Gutachten der Stiftung Familienunternehmen und Politik wird mehr Datenschutz gegenüber mehr Transparenz gefordert. Im Grundsatz geht es um den Einblick in das Transparenzregister, in dem jeder Bürger mit einer Unternehmensbeteiligung von > 25% als wirtschaftlich Berechtigter mit Namen, Geburtsdatum, Nationalität und Aufenthaltsort gemeldet sein muss. „Verbunden mit anderen Pflichtveröffentlichungen, bekommen Außenstehende tiefe Einblicke in die Unternehmensführung und das Privatleben.“ Es gehe nicht an, wie der EuGH im November 2022 feststellte, dass jeder ohne ein nachgewiesenes, berechtigtes Interesse Einsicht bekommen kann.³¹ Wie hatte es der Datenschutzbeauftragte für Hamburg (HambBfDI) so treffend in seinem Tätigkeitsbericht für 2022 festgehalten:³²

„Nicht der Datenschutz erschwert die Digitalisierung, sondern schlechte Digitalisierung erschwert guten Datenschutz.“



(b) Ist der Steuerberater Auftragsverarbeiter nach DS-GVO?

Eine bisher gern diskutierte Frage und wer sucht, der findet auch ... in der Auslegungshilfe des Bay. Landesamtes für Datenschutz.³³ Kurz gesagt: „Nein“ Begründung: Aufgrund des Steuerberaterrechts handeln diese in eigener Verantwortung und können deshalb keine Leistung nur auf Weisung ihrer Mandantschaft erbringen. Zitat:

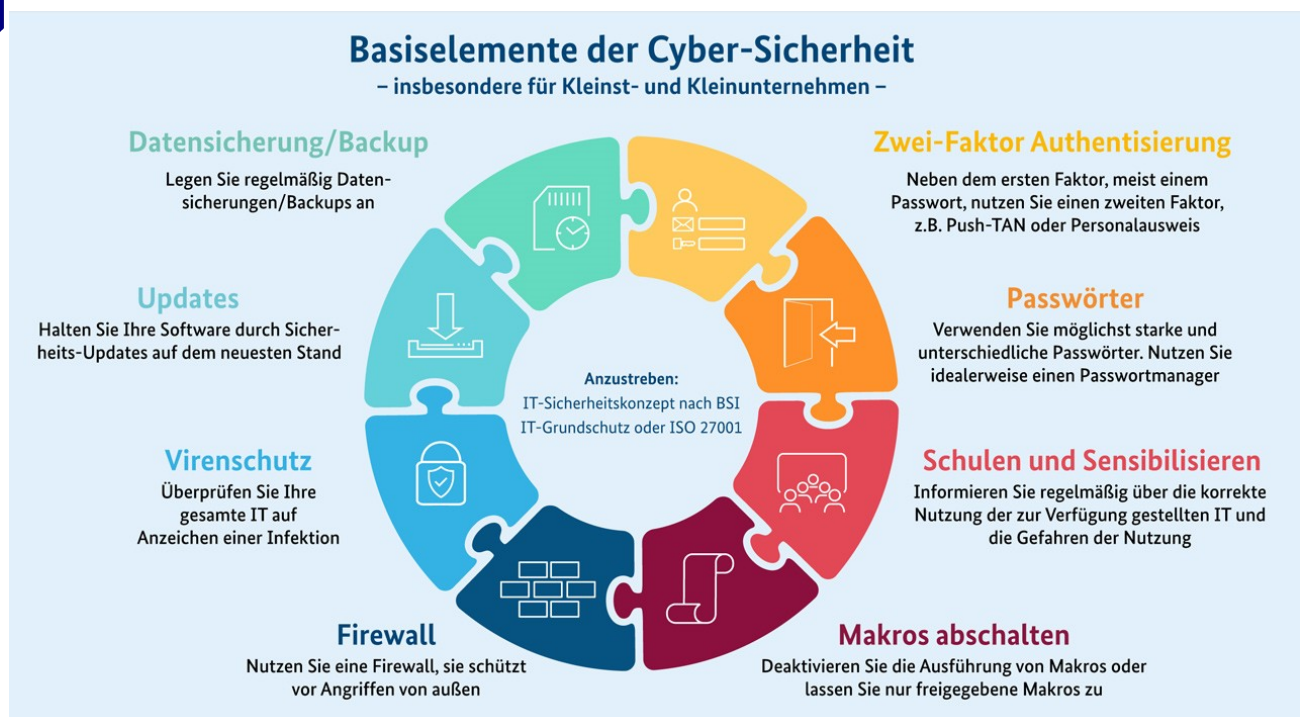
Steuerberaterinnen und Steuerberater arbeiten deshalb aus unserer Sicht regelmäßig eigenverantwortlich aufgrund eines Mandantenvertrags und dürfen von der Mandantschaft im Rahmen der Erforderlichkeit für ihre Tätigkeit im Sinne von Art. 6 Abs. 1 Satz 1 lit. f DS-GVO personenbezogene Kunden- und/oder Beschäftigtendaten erhalten.

(3) Zur Datensicherheit

(a) Einstieg Cybersicherheit



i) Basiselemente (Infografik)



Quelle: Bundesamt für Sicherheit in der Informationstechnik



ii) Datensicherung/Backup

➤ Wann sind Sicherheitskopien die Rettung?

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 10/28

- | | | |
|-----------------|---|--------------------------|
| 1. Bei Defekt | 3. Bei verschiedenen Schadprogrammen | 5. Bei Gerätediebstahl |
| 2. Bei Löschung | 4. Bei Gebäudeschäden / Naturkatastrophen | 6. bei Cloud – Problemen |

➤ Was soll gesichert werden?

1. Das Betriebssystem, wenn die individuelle Konfiguration nicht verloren gehen soll
2. Die Anwendungsprogramme, wenn die individuelle Konfiguration nicht verloren gehen soll
3. Die Anwendungsdaten auf jeden Fall, denn diese sind sonst verloren, dafür gibt es keine Standard-Wiederherstellungsfunktion.

➤ Wie soll gesichert werden?

- ▶ Volldatensicherung *Für jede Sicherung werden sämtliche Daten gesichert
(+) Alles gesichert (-) Könnte viel Platz und Zeit brauchen*
- ▶ Inkrementelle Datensicherung *Nach einer Volldatensicherung werden mit jeder weiteren Sicherung nur die Veränderungen zu vorgehenden Sicherung gespeichert. (+) Spart Kapazitäten und Zeit (-) Rücksicherung nur mit allen Teilsicherungen*
- ▶ Differentielle Datensicherung *Nach einer Volldatensicherung werden bei jeder Sicherung alle Änderung zur Ursprungssicherung gespeichert. (+) Die Wiederherstellung ist unkomplizierter (-) Braucht mehr Kapazitäten und Zeit als die Inkrementelle Sicherung.*
- Durchführung *Mit Windows kann über die Systemsteuerung > Alle Systemsteuerungselemente >Wiederherstellung eine Sicherung konfiguriert werden, oder man nutzt eine Software (Vereinfachung bei Netzwerken mit Client und Servern), mit der eine Wiederherstellung auch notfalls auf einer anderen Hardware vorgenommen werden kann. In jedem Fall auf einem externen Medium oder in der Cloud. Dann allerdings verschlüsselt vor Übertragung (Beispielhaft eine Übersicht im Testvergleich³⁴)*



iii) Updates

Updates dienen zwar auch dazu, einer Software neue Funktionen hinzuzufügen, ohne diese neu installieren bzw. aufsetzen zu müssen. Viel wichtiger sind aber die Sicherheitsupdates, mit denen Schwachstellen im System geschlossen werden, die sonst Hacker für Angriffe nutzen. Checkliste:

- Liste der Programme, die eine Auto-Update-Funktion anbieten und eingeschaltet sind.
- Liste der Programme, die manuell aktualisiert werden müssen.
- Updates immer sofort installieren (!!!)
- „Vertrauen ist gut, Kontrolle ist besser“, informiert bleiben.
Der BSI stellt verschiedene Newsletter zur Verfügung u. a. zu BCM (Betriebl. Kontinuitätsmanagement), Cloud-Computing, IT-Grundschutz, KMU und Verbraucherschutz³⁵.



(4) Zu angrenzenden Themen

(a) April: Updates, Updates, Updates!

Nachdem vor der aktuellen Situation auch staatliche Hacker massiv unterwegs sind, versuchen auch die Hersteller verstärkt mögliche Sicherheitslücken zu finden und alle bekannten Lücken zu schließen. Ob Betriebssystem (Windows, Apple, Linux), Browser (Edge, Firefox, Chrome, Safari u. a.), Kollaborationssoftware (Zoom, Webex, Skype, Teams u.a.), viele beliebte Anwendungen und Hardwaretreiber für Prozessoren, Router, Grafikkarten, es gibt eine Vielzahl von Ankündigungen zu Sicherheitsupdates in diesem Monat. So viele Links kann ich hier nicht verknüpfen, ohne die 3. Seite zu sprengen. Vorschlag: Nach Möglichkeit den Status der Anwendungen und Treiber graduell prüfen.

PS: Bevor jetzt der Hinweis kommt, warum Apple und Linux, hier nur zwei aktuelle Hinweislinks:

- > [Linux Kernel KVM: Schwachstelle ermöglicht Codeausführung](#)
- > [LockBit crew cooks up half-baked Mac ransomware](#)

★ 05@2023

(2) Zum Datenschutz



(a) Whistleblower und Datenschutz (jetzt doch)

Die Umsetzungspflicht aus der EU – Whistleblower – Richtlinie (EU-Richtlinie 2019/1937³⁶) hätte bis zum 17.12.2021 in lokales Recht umgesetzt werden müssen. Das Bundeskabinett ist dem im ersten Halbjahr 2022 mit dem Hinweisgeberschutzgesetz (HinSchG)³⁷ nachgekommen, zunächst aber im Bundesrat gescheitert. Verabschiedet wurde es dort jetzt im Mai 2023³⁸ und tritt 4 Wochen nach Veröffentlichung im Bundesgesetzblatt in Kraft (Juni/Juli 2023). Das Hinweisgeberschutzgesetz ergänzt bestehende, gesetzliche Regelungen (Geldwäsche, Kreditwesen, Wertpapiere, Versicherung, Börse, Wirtschaftsprüfung, Marktmissbrauch, Verkehr, nationale Sicherheitsinteressen, Verschwiegenheits- und Geheimhaltungspflichten u. ä.). Ziel ist eine bessere Durchsetzung des Rechts in Deutschland und Europa zum Schutz von Leben, Leib, Gesundheit, Beschäftigten und / oder ihrer Vertretungsorgane. Mit den Mindeststandards soll ein hohes Schutzniveau für Personen erreicht werden, die im Zusammenhang mit ihrer beruflichen Tätigkeit (Arbeitnehmer*/innen, Beamte*/innen, Selbstständige, Anteilseigner*/innen oder Mitarbeiter*/innen von Lieferanten) Informationen über Verstöße erlangen und diese melden.



i) **Whistleblower (Hinweisgeber)**

Hinweisgeber sind natürliche Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese an die nach diesem Gesetz vorgesehenen Meldestellen melden oder offenlegen (§1 HinSchG). Für die Informationsbeschaffung besteht ein Ausschluss der Verantwortlichkeit (§36 HinSchG). Die Informationen dürfen allerdings nicht unter einem eigenständigen Straftatbestand beschafft worden sein. Falschinformation sind schadenersatzpflichtig.



ii) **Schutz des Hinweisgebers**

Nach dem Vertraulichkeitsgebot in den §§8, 9 HinSchG ist die Identität des Hinweisgebers zu wahren. Ausnahmen bestehen ausschließlich für Straf- und Bußgeldverfahren, gerichtliche Entscheidungen, BaFin, Bundeskartellamt und bei Erforderlichkeit zur Ergreifung von Folgemaßnahmen und bei Einwilligung.

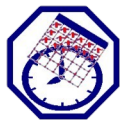


iii) **Meldestellen**

Unternehmen und Organisationen ab 50 Beschäftigten müssen sichere, interne Hinweisgebersysteme installieren und betreiben. Die Organisation der Meldestelle kann nach §14 HinSchG auch an Dritte ausgelagert werden (die Verantwortung bleibt bestehen). Daneben gibt es externe Meldestellen beim Bundesministerium der Justiz, BaFin, Kartellamt, Finanzämter u.ä.).

iv) **Meldungen**

Es muss die Möglichkeit bestehen, Meldung mündlich, schriftlich oder auf Wunsch persönlich abzugeben. Anonyme Meldungen sollen aber auch bearbeitet werden. Es besteht die freie Entscheidung, wo eine Meldung abzugeben ist, dabei sind interne Meldestellen zu bevorzugen.



v) **Fristen**

Eine Eingangsbestätigung muss innerhalb von 7 Tagen bestätigt werden und binnen 3 Monaten ist der Whistleblower über die ergriffenen Maßnahmen zu informieren. Es besteht Dokumentationspflicht.

vi) **Repressalien; Beweislastumkehr**

Repressalien gegen Whistleblower sind verboten, auch schon die Androhung und begründen einen Schadenersatzanspruch (§37 HinSchG). Der Gegenbeweis ist von der Organisation / dem Unternehmen zu erbringen (Beweislastumkehr §36 HinSchG).



(b) **Hinweisgeber im Datenschutz (VVT)**

Eine gute Vorlage ist die Orientierungshilfe zu Whistleblower-Hotlines der Datenschutzkonferenz der Aufsichtsbehörden (DSK) aus Ende 2018³⁹. Zur Einordnung nach den Vorschriften zum Verzeichnis der Verarbeitungstätigkeiten (Erläuterung Fußnote⁴⁰):

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

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

- ▶ Zugriff, wer verarbeitet die Daten:

Nur unabhängige, mit der Aufgabe betraute, fachkundige Mitarbeiter/innen (§15 HinSchG).

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

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

- ▶ **Rechtsgrundlage, Löschrufen, Besonderheiten:**

Rechtsgrundlage ist die Verpflichtung nach dem HinSchG ([Art.6 Abs.1c DSGVO](#)). Löschrufen bzw. Aufbewahrungspflicht: 2 Jahren nach dem [HinSchG §11 Nr. \(5\)](#). Besonderheiten: Die Informationspflicht an einen Beschuldigten besteht nicht, wenn eine wirksame Untersuchung dadurch behindert wird. Die Besonderheiten für Empfänger, Transfer, Drittland u. ä. sind zu beachten.



- ▶ **Schutzkonzept**

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

- ▶ **PS:** Das Schutzkonzept sollte die Eintrittswahrscheinlichkeit deutlich reduzieren. Bei unverändert hohem Risiko (Schadenpotential x Eintrittswahrscheinlichkeit) ist eine Vorstellung bei der Aufsichtsbehörde vorab vorzunehmen ([Art.36 DS-GVO](#); zur Risikoabwägung siehe Fußnote⁴¹, Zusammenfassung SDM, Seite 7).

(3) Zur Datensicherheit

(a) Virenschutz

Dass ein Schutzprogramm / Virens Scanner unverzichtbar ist, zeigen die aktuellen bis täglichen Warnung und die Vielzahl der wichtigen „Systemupdates“ zum Schutz vor bekannten Schadprogrammen.

i) **Gratis oder kostenpflichtig**

Wie immer, ist es eine Frage der Anforderungen. Wie aktuelle Testbewertungen zeigen, kann eine Gratis - Version für einen Einzelplatzrechner oder Mobilgerät ausreichend sein. Ein Blick auf die Auswertungen des unabhängigen, Magdeburger AV - Test Instituts⁴² kann bei der Entscheidung hilfreich sein. Geht es an Mehrplatzrechner oder Client – Server – Strukturen mit Fernzugriff, vielleicht noch über Drittgeräte, sollte ein Spezialist mit entsprechendem Support hinzugezogen werden. Hilfestellung zum Einstieg gibt es auch vom BSI unter: „[Wie Sie Ihren Computer sicher einrichten](#)“.



ii) **Online - Virens Scanner**

Es erscheint zunächst leichter, da keine Installation erforderlich und immer die aktuellste Prüfroutine genutzt wird. Allerdings fehlt der Wächter im Hintergrund, der jede aufgerufene Datei auf Signaturen prüft, er steht Offline nicht zur Verfügung, erfordert die Ausführung aktiver Inhalte (ActiveX) und muss möglicherweise über eine infizierte Onlineverbindung genutzt werden. Nützlich kann ein Onlinescanner helfen, wenn auf einem ungeschützten Rechner eine Infizierung vermutet wird oder für Einzelprüfungen, wie bei VirusTotal (Zusammenschluss von 70 Anbietern)⁴³.



iii) **Empfehlung(en)?**

Ein Virens Scanner muss tief in die Systemarchitektur eingreifen können und sollte langfristig eingesetzt werden. Deshalb sind strenge Kriterien anzulegen und neben der Software sollte auch der Anbieter kritisch unter die Lupe genommen werden.

★ **06@2023**

(2) Zum Datenschutz



(a) Videoüberwachung, verboten, erlaubt?

Grundsätzlich gelten die Vorschriften der [DS-GVO Art.6](#) für eine rechtmäßige Erhebung von Videoaufzeichnungen (Einwilligung, Vertragserfüllung, rechtliche Verpflichtung, lebenswichtige Interessen, im öffentlichen Interesse, oder im berechtigten Interesse des Verantwortlichen).

i) *Haushaltsausnahme*

Diese gilt für den privaten Bereich, sofern keine Dritten hiervon betroffen sind (z. B. Nachbargrundstück, öffentliche Bereiche, ausnahmslos für den privaten, persönlichen Bereich). Social - Media zählt nicht zum privaten Bereich und das Urheberrecht ist auch zu beachten.



ii) *Berechtigtes Interesse des Verantwortlichen (Art. 6 Abs. 1f)?*

Dazu hat der europäische Datenschutzausschuss (edpb)⁴⁴, wie die Datenschutzkonferenz der Länder (DSK)⁴⁵ bereits Handlungs- bzw. Orientierungshilfen veröffentlicht. Vereinfacht gilt: „Einfach so geht nicht!“ und die Schutzinteressen der betroffenen Person dürfen nicht überwiegen. Es muss eine reale Gefährdungslage vorliegen, z. B. Vandalismus im öffentlichen Nahverkehr, schwere Vorfälle in der Vergangenheit, oder Diebstähle in Einkaufszentren u.ä. Vor Zutritt ist ein deutlicher Hinweis auf die Pflichtinformationen anzubringen ([LDI-NRW Muster: „Vorgelagertes Hinweisschild“](#)).



iii) *Verdeckte Videoüberwachung?*

Das Bundesdatenschutzgesetz hält in [§32 Abs.1 Nr.4](#) fest, dass eine Ausnahme zur Informationspflicht besteht, wenn diese die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen überwiegen. Nach Auffassung des Bundesarbeitsgerichts ([BAG 2 AZR 395/15](#)) ist eine verdeckte Videoüberwachung zulässig, wenn

- (a) der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht und
- (b) ein begründeter Verdacht auf einen räumlich und funktional abgrenzbaren Bereich besteht (keine Mutmaßungen) und
- (c) weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind und
- (d) die Überwachung insgesamt nicht unverhältnismäßig ist.

Eine hinreichende Abwägung und Dokumentation ist in jedem Fall im Vorfeld erforderlich.



(b) *Mitarbeiterkontrolle?*

Wo „wir“ gerade bei Mitarbeiter sind. Die rechtlichen Grenzen der Kontrollen stellen die individuellen Rechte, die Mitbestimmung des Betriebsrats und natürlich der Datenschutz dar. Haufe.de gibt in einem Artikel dazu eine Übersicht⁴⁶. Die Kernaussagen:

- Ob erlaubt oder nicht, die inhaltliche Kontrolle der privaten E-Mail und Internetnutzung ist alleine aufgrund des Fernmeldegeheimnisses nicht erlaubt (Ausnahme: Straftatverdacht / Notfälle)
- Einsatz von Keyloggern / Screenshots auf Dienstcomputern ohne Einwilligung ist nicht erlaubt. (Ausnahme: Straftatverdacht)
- Offene Kameraüberwachung ist für einen legitimen Zweck am Arbeitsplatz erlaubt, sofern diese den Mitarbeiter nicht schikaniert, oder unter Druck setzt und verhältnismäßig ist.
- Die Nutzung von Standortdaten (GPS, Firmensmartphone u.ä.) ist nur unter sehr engen Grenzen erlaubt und nicht ohne Wissen des Mitarbeiters.
- Für das Home - Office gibt es kein Zutrittsrecht und der Überwachung durch einen Privatdetektiv sind sehr enge Grenzen gesetzt (Straftatverdacht, konkrete Betrugsverdacht).

(3) *Zur Datensicherheit*



(a) *Basiselemente der Cyber-Sicherheit*⁴⁷ **Nr. 4 Firewall**

Abgeleitet von der Brandschutzwand oder -tür, blockiert bzw. schützt es das Netzwerk (meist eine Kombination aus Hard- und Software) und/oder den einzelnen Rechner (Personal Firewall) vor allen Zugriffen von außen, wie vor anderen Geräten und Netzwerken (u. a. dem Internet). Die Firewall erkennt nicht, ob der Zugriff harmlos oder feindlich ist. Sie erlaubt oder verbietet den Datenverkehr mit der anderen Stelle. Deshalb ist die Kombination mit einem zuverlässigen Antivirenprogramm wichtig, dass installierte Anwendungen, wie dynamische Webseiteninhalte auf Gefahren prüft (Security Pakete).



i) *Software Firewall*




Für einen ersten Eindruck der Funktionsweise rufen Sie z. B. in Windows die Einstellungen zur Firewall auf. In Windows über die Suche (🔍) und Eingabe „Firewall“ mit der Auswahl „Windows

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 14/28

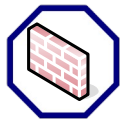
Defender ...“ In der folgenden Übersicht erscheinen 3 Kategorien mit unterschiedlichem Sicherheitsniveau.

- A. ▶ „Domänenprofil“, für Netzwerke mit Kontoauthentifizierung.
- B. ▶ „Privates Profil“, für Heimnetzwerke u. ä.
- C. ▶ „Öffentliches Profil“, für öffentliche Netzwerke wie Hotspots in Cafés, Hotel, Geschäften u.s.w.

In den empfohlenen Einstellungen sollte:

- D.  Die Firewall aktiviert sein
- E.  Eingehende Verbindungen ohne Regel werden blockiert
- F.  Ausgehenden Verbindungen ohne Regel werden zugelassen.

➔ Über Firewall Eigenschaften werden die Einstellung dazu angezeigt. Hinweis: In den Einstellungen sollte „Benachrichtigungen anzeigen“ auf „Ja“ eingestellt sein. Wenn die Firewall eingehende, wie auch ausgehende Verbindungen je nach Einstellung blockiert, wird eine Nachricht angezeigt und je Einzelfall kann mit Rechten als Administrator eine Freigaberegul für vertrauensvolle Verbindungen erstellt werden.



ii) Hardware Firewall

Die Bezeichnung ist nicht ganz korrekt, ohne Software funktioniert keine Firewall, diese Bezeichnung besagt lediglich, dass die Firewall (Software) unabhängig vom Client / Server auf einem externen Gerät (z. B. Router) läuft und den gesamten Datenverkehr kontrolliert. So liegen z. B. die Zugangsdaten für die Netzwerke separat auf dem externen Gerät. Die Funktionen sind⁴⁸:

- **Paketfilter:** Prüft die Header – Informationen und lässt das Paket durch, oder eben nicht.
- **Stateful – Packet – Inspection:** Eine dynamische Filtertechnik, bei der jedes Datenpaket einer bestimmten aktiven Session zugeordnet wird.
- **Proxyfilter:** Als „Stellvertreter“ wird neben Adress- und Protokolldaten auch der Datenverkehr auf Anwendungsebene analysiert. Ergänzt um einen „Contentfilter“ können auch unerwünschte Inhalte aus Webseiten (z. B. ActiveX, JavaScript u.ä.) einschließlich ganzer Webseiten herausgefiltert werden.
- **Deep Packet Inspection:** Hier werden nicht nur Ursprung und Ziel (Header), sondern auch der Inhalt analysiert, wodurch sich intelligentere Regeln aufstellen lassen. Um verschlüsselte Pakete analysieren zu können, ist zusätzlich eine SSL-/TLS-Termination erforderlich, die das Paket anhält, entschlüsselt und nach Analyse wieder eine verschlüsselte Verbindung zur Zieladresse aufbaut.



iii) Und jetzt?

Eine Empfehlung kann ich natürlich nicht aussprechen, da dies von der jeweiligen Konstellation abhängig ist. Einen IT – Spezialisten um Rat fragen, kann sicher nicht schaden. Hilfreich ist ggf.:

- **Anleitung:** „Bewährte Methoden zum Konfigurieren von Windows Defender Firewall“ Microsoft.⁴⁹
- **Zur einfachen Konfiguration** der Personal Firewall mit einer gut verständlichen und deutschsprachigen Oberfläche empfiehlt chip.de, z. B. die „Free Firewall“⁵⁰ der IT-Beratung Steinmiller aus Kraichtal.
- **Vergleich Security Pakete:** Firewall Vergleich 2023 mit Erläuterungen auf verlgeich.org⁵¹
- **BSI:** Basis zur IT-Sicherheit: „Firewall“ und der Baustein NET.3.2: Firewall (Edition 2021)⁵²

★ 07@2023

(2) Zum Datenschutz



(a) EU – US – Data – Privacy - Framework: Fluch oder Segen?

Von heller Begeisterung (Bitkom: „Dreijährige Hängepartie geht zu Ende“)⁵³ bis erneute Klage vor dem EuGH (noyb/Schrems: „Kopie des gescheiterten „Privacy - Shields“)⁵⁴ reichen die Reaktionen auf den dritten Anlauf.



i) Warum die Aufregung?

Für einen Datentransfer in ein Drittland (zur EU) gilt der Grundsatz: „Der Datenschutz reist mit den Daten!“ ([Kurze Checkliste habe ich hier als PDF verlinkt](#)). Die einfachste Prüfung ist die Vorlage

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 15/28

eines [EU - Angemessenheitsbeschlusses](#), d. h. die EU hat die Angemessenheit des Datenschutzes nach DS-GVO geprüft. Für US-Unternehmen braucht es nur noch eine Zertifizierung nach dem Trans – Atlantic – Data – Privacy - Framework und der Datentransfer ist mit dem Datenschutz nach DS-GVO vereinbar.



ii) Wo ist das Problem?

Noyob schreibt dazu u. a., dass der EuGH bereits feststellte, dass die Massenüberwachung (von Nicht-US-Bürgern) nach dem „[Foreign Intelligence Surveillance Act \(FISA\), Section 702](#)“ nicht verhältnismäßig ist, der Rechtsbehelf über den Ombudsmann würde nicht im Entferntesten dem [Artikel 47 der EU - Grundrechtecharta](#) entsprechen und im Übrigen wäre das neue Abkommen eine Kopie von 2016. Internet World schreibt dazu: „Das EU-US-Datenschutzabkommen ist völlig wertlos, ein Fiasko für die Wirtschaft“⁵⁵.



iii) Und jetzt?

Positiv zu vermerken bleibt die Reaktion des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit⁵⁶:

„Mit dem neuen Angemessenheitsbeschluss können ab sofort personenbezogene Daten aus der EU an die USA wieder fließen, ohne dass weitere Übermittlungsinstrumente oder zusätzliche Maßnahmen erforderlich sind. Dies gilt jedoch nur, sofern die Organisation, an die sie übermittelt werden, auch unter dem EU - U.S. Data – Privacy - Framework zertifiziert ist.“

Nach den jetzt gültigen Regelungen kann mit einem zertifizierten US-Unternehmen ein Datentransfer vorgenommen werden. Allerdings können die letzten Zweifel erst ausgeräumt werden, wenn der EuGH dazu angerufen wurde und sein Urteil verkündet. Es bleibt also in den nächsten Jahren zu beobachten und Zeit, um einen Notfallplan B für den Fall der Fälle ins Auge zu fassen, oder gleich eine, der sichere Alternativen zu wählen.

(3) Zur Datensicherheit

(a) Basiselemente der Cyber-Sicherheit Nr. 5 „Makros“

Makros können ein Segen sein, um sich wiederholende, regelmäßige Vorgänge mit einem Klick (Makro) auszuführen. Leider können solche Makros auch ein Fluch sein, denn es lassen sich auch ganze Programme darin „verstecken“. Wie dem ESET Threat Report H1 2023⁵⁷ zu entnehmen, gehörten Office-Makros über viele Jahre zu den größten Cyberbedrohungen global. Mittlerweile hat Microsoft in den Standardeinstellungen Makros deaktiviert. Neben den selbst erstellen Makros besteht die Gefahr, schädliche Makros von Dritten über E-Mail und Dateianhängen, Download, Erweiterungen (Addons), Programminstallation u. ä. zu erhalten. Makros können auch in anderen Dateien (z.B. PDF) versteckt sein. Wie immer ist die Konfiguration ein Kompromiss aus Sicherheit versus Komfort und Funktionalität.



i) Sicherheitseinstellungen einordnen



Sehr hoch

Nur Makros aus vertrauenswürdigen Dateiquellen werden ausgeführt. Alle anderen Makros werden deaktiviert, unabhängig von einer Signatur.



Hoch

Nur signierte Makros aus vertrauenswürdigen Quellen werden ausgeführt. Nicht signierte Makros werden deaktiviert.



Mittel

Bestätigung vor dem Ausführen von Makros aus nicht vertrauenswürdigen Quellen.



Niedrig

Alle Makros ausführen ist nicht empfehlenswert, nur wenn sichergestellt ist, dass nur sichere Dokumente geöffnet werden können.



ii) Und jetzt?

Gute und vertrauenswürdige Programmanbieter haben die Ausführung von Makros bereits in den Voreinstellungen deaktiviert und geben einen Warnhinweis vor Aktivierung aus. Ein Blick in Office und Kommunikationsanwendungen ist sicher hilfreich und beruhigend (meist unter „Trust Center, Sicherheit und Datenschutz u. ä.).

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 16/28

Für mittelgroße und große Organisationen, die Endsysteme mit Gruppenrichtlinien in einer Active – Directory - Umgebung verwalten, gibt die BSI Empfehlungen mit Schwerpunkt auf Microsoft Office Anwendungen⁵⁸. Die zur Weitergabe an den IT – Service (bzw. Dienstleister) sehr zu empfehlen sind.

(4) Zu angrenzenden Themen



(a) EU – DATA - ACT, was ist das denn jetzt?

Es geht um „freie Daten für den Wirtschaftsaufschwung“⁵⁹, mit Schwerpunkt auf die breite Nutzung von Daten vernetzter Geräte, wie Sprachboxen, Smartwatches, E-Autos, Smart-Home-Systemen bis hin zu industriellen, wie landwirtschaftlich genutzten Geräten und Robotern. Es besteht die Pflicht, Gerätedaten (ohne Personenbezug) von technischen Geräten zur Verfügung zu stellen.



i) Die guten Nachrichten:

- ✓ Wie bei der DS-GVO sind Kleinunternehmen (weniger als 50 Personen, weniger als € 10 Mio. Umsatz) ausgenommen.
- ✓ Verbraucher, wie Unternehmen können von Dateninhabern neben den personenbezogenen Daten nach [Art.20 DS-GVO](#), auch die Herausgabe der nicht personenbezogenen Gerätedaten verlangen (Art.5 EU-Data-Act) und in Eigenverantwortung auch weitergeben.
- ✓ Das EU-Gesetz zielt auch darauf ab, die Dominanz der US-amerikanischen Technologiegiganten einzudämmen: Große Cloud-Anbieter, wie Amazon Web Services, Microsoft und Google werden demnach dazu verpflichtet, illegalen Zugriff auf Daten zu verhindern und Standards für einen erleichterten Anbieterwechsel zu etablieren.



ii) Konflikte:

- x Es besteht sogar die Pflicht des Dateninhabers seine Daten mit Dritten zu teilen, also Schnittstellen zum leichteren Austausch zu schaffen. ABER, diese Daten dürfen keine Rückschlüsse auf Personen zulassen (DS-GVO), sind also zu anonymisieren, eine Pseudonymisierung (Personenbezug in separater Speicherung) ist nicht erlaubt.
- x Es besteht die Befürchtung, Geschäftsgeheimnisse könnten durch die Pflicht zur Datenweitergabe in Gefahr geraten. Die Offenlegung von Daten zu Geschäftsgeheimnissen besteht ausdrücklich nicht. Für Streitigkeiten soll eine zugelassene Stelle zur Beilegung von Streitigkeiten angerufen werden (Art.10 EU-Data-Act).
- x Es bleibt wenig Zeit, da der Data - Act nach 20 Monaten inkrafttreten soll.

Ohne tief in die Thematik eingestiegen zu sein, würde ich sagen: „Da ist noch viel Musik drin, für die Unternehmen, die es anwenden müssen“.

★ **08@2023**

(2) Zum Datenschutz



(a) Verein: Mitgliederlisten & Datenschutz

Wer darf Mitgliederlisten mit Kontaktdaten einsehen und erhalten? Wird da nicht oft der Datenschutz vorgeschoben, weil man es nicht will? Aus einem Urteil des OLG Hamm 8 U 94/22 vom 26.04.2023⁶⁰. Gestützt auf [Art.6 Abs.1b\) DS-GVO](#) (erforderliche Verarbeitung aus Vertrag) darf:

- ✓ Der Vorstand zur Information der Mitglieder über vielfältige Themenbereiche, insbesondere für eine korrekte Einladung zur Mitgliederversammlung, Trainer / Gruppenleiter für ihre jeweilige Untergruppe. Alle Zugriffe im Sinne der rechtmäßigen Ausübung von Vereinsleistungen und Veranstaltungen.



Den Mitgliedern zur Kontaktaufnahme mit anderen Mitgliedern?

- ✓ JA, aus der besonderen (Vereins-) Beziehung der Mitglieder untereinander
- ✓ WENN keine anderen, überwiegenden Interessen dagegen stehen.
- ✓ NICHT mit einer werblichen Ansprache im Sinne des UWG verbunden ist.

„DS-GVO Art.6 Abs.1 f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen

oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.“

Dabei ist durch die Verantwortlichen immer einer Interessenabwägung durchzuführen. Wirksame Widersprüche einzelner Mitglieder müssen individuell begründet sein (z.B. Feindschaft mit, oder Stalking durch ein anderes Mitglied) und dargelegt werden.



(b) Dateneigentum (!?)

Mit dem EU – DATA - ACT (freie Daten für den Wirtschaftsaufschwung) „geistert“ gerade im Widerspruch die Idee vom Eigentum an Daten durch die Fachpresse. Detaillierte Auseinandersetzung mit dem Thema im CMS Deutschland Blog „Data Ownership – Keine Eigentumsrechte an Daten“⁶¹.

Mit personenbezogenen Daten geht es mit der DS-GVO schon mal nicht. Es kann zwar ein Nutzungsrecht nach den Vorgaben der DS-GVO vereinbart werden („Einwilligung“ u.s.w.), allerdings muss dieses Nutzungsrecht auch jederzeit widerrufbar sein und bleiben.

Übrig bleiben also die „unpersönlichen Maschinendaten“. So kommt auch eine Arbeitsgruppe des Bundesministeriums für Wirtschaft und Energie zu der Erkenntnis:

„Eine generalisierte Zuweisung von Ausschließlichkeitsrechten an Daten, ohne zugleich diese Rechtsposition wieder relativierende Zugangs- und Teilhaberechte zu regeln, birgt ein hohes Risiko, vor allem innovationshemmend zu wirken und den gewünschten „Free Flow of Data“ erst gar nicht entstehen zu lassen.“⁶²

Mit anderen Worten, folgt man dem Gedanken des EU – Data – Acts, dann erfordern neue Technologien eine offene Gesellschaft und Informationen sind für die Informationsgesellschaft zu wichtig, um sie einer Eigentumsposition mit Exklusivrechten zuzuordnen.

(3) Zur Datensicherheit



(a) Basiselemente der Cyber-Sicherheit Nr. 6 Schulen & Sensibilisieren

Ein wichtiger Sicherheitsfaktor zur Abwehr von Cyberangriffen ist der Mensch (*und nicht das Problem, um es mal deutlich zu sagen, denn nur Mensch kann noch verhindern, was die IT-Sicherheit nicht kann.*). Damit er diese Anforderung meistern kann, sollte der Mensch regelmäßig sensibilisiert und geschult werden.



i) Information & Unterstützung durch:

- ✓ Verständliche Information über die technischen Sicherheitsvorkehrungen, deren Schutzwirkung und vor allem über deren Grenzen!
- ✓ Vermittlung eines guten Gefühls bei verdächtigen Aktivitäten (z. B. E-Mail) lieber eine Anfrage zu viel den IT-Verantwortlichen vorzustellen, als genau die „EINE“ zu wenig.
- ✓ Einfache Tipps, wie z.B. den 3-Sekunden-Sicherheits-Check⁶³ des BSI zu E-Mails (1. Kenne ich den Absender? 2. Ist der Betreff sinnvoll? 3. Erwarte ich den Anhang?) PLUS: 4.) Fehler im Text und sichtbare Links weichen von echtem Link ab (z.B. „google.com“ zu „gooogle.com“).
- ✓ Wenige Grundregeln in der E-Mail Kommunikation erhöhen nicht nur die Effizienz, sondern auch die Sicherheit zur Erkennung korrekter E-Mails. Zum Beispiel die Vermeidung unnötiger „Empfänger in „cc & bcc“, ein kurzer Betreff beginnend mit dem Grund (INFO: AUFGABE: ANTWORT: EILT: ERLEDIGT:) „|“ Termin(e) „|“ mit Stichwort zum Thema und bei jeder E-Mail vom Absender im 1. Absatz eine kurze Zusammenfassung der Erwartung an den / die Empfänger zur Mail.
- ✓ ...



ii) Informationen zu Angriffsflächen

- ✓ Um eine möglichst realitätsnahe Nachricht zu erstellen, sammeln Betrüger Informationen in sozialen Netzwerken und auf Plattformen. Deshalb ist mit persönlichen und geschäftlichen Informationen dort sehr verantwortungsvoll umzugehen. Keine Veröffentlichung von vertraulichen Informationen in sozialen – Netzwerken und überhaupt in der Kommunikation mit Dritten über den Arbeitgeber, die Organisation und die Arbeit.

- ✓ Zugangsdaten, Passwörter oder Kontoinformation niemals per Mail, Telefon oder Konferenzsystemen weitergeben, da die Gefahr des Mitlesens oder Mithörens besteht.
- ✓ Betrüger nutzen auch gerne Fernwartungssoftware (Remote – Services), um sich auf den eigenen Rechner aufzuschalten und durch Ablenkung Schadsoftware aufspielen zu können. Der 3-Punkte-Check vor Einsatz von Fernwartungssoftware 1.) Ist der Anbieter bekannt? 2.) Besteht eine Vereinbarung mit dem Serviceanbieter? 3.) Ist die Rechtmäßigkeit einer Ankündigung auf unabhängigem Kommunikationsweg bestätigt?
- ✓ „Wie Hacker Ihre Psyche entschlüsseln ... und wie Sie sich davor schützen können. Psychotricks und Phishing-Maschen“ ein DIN A3 Poster der Allianz-für-Cybersicherheit⁶⁴ zeigt kurz und übersichtlich die Tricks und Maschen der Kriminellen. Ein Aushang kann die Aufmerksamkeit hochhalten.



iii) „Outdoor – Office“

Auch wenn hinlänglich beschrieben, geschrieben, gesagt und gezeigt, fällt mir beim Reisen doch immer wieder auf, dass ein Minimum an Grundregeln nicht beachtet wird.

- SPERREN: Geräte sollten zwar nie unbeaufsichtigt sein, aber sobald man es „aus der Hand“ legt ist die Sperre (Passwort oder biometrische Sperren u. ä.) auf Smartphone, Laptop umgehend zu aktivieren.
- NETZ: Öffentliche WLAN – Netze sind immer ein Risiko für und mit sensiblen Daten. „Wenn es denn sein muss, nie ohne VPN (Virtual Privat Network; verschlüsselte Verbindung zwischen zwei Beteiligten). Im Zweifel lieber auf das Mobilfunknetz setzen, z. B. über die einen WLAN - Hotspot vom Smartphone mit VPN. Anleitung zur Ersteinrichtung von chip.de⁶⁵
- VERSCHLÜSSELN: Damit im „Fall der Fälle“ kein unerlaubter Zugriff auf Rechner oder Smartphone erfolgt, ist eine Verschlüsselung angebracht, die meistens schon „an Board“ ist, mit BitLocker bei Windows, FileVault bei Mac-OS. Die Smartphones, iPhones wie Android ab Version 10 sind standardmäßig verschlüsselt.
- DISKRETION: „Mithören“ und „Mitsehen“ lässt sich in öffentlichen Räumen auch für Dritte meist schlecht vermeiden. Deshalb keine Telefonate oder Videokonferenzen zu vertraulichen Themen und Nennung von Namen / Daten / Fakten. Hilfreich ist auch eine Blickschutzfolie zur Vermeidung neugieriger Blicke.
- NIE KIOSK-PCs: ... an Flughäfen oder in Hotels, wie unbekannte Hardware Dritter für Dienste mit sensiblen Inhalten und Zugangsdaten nutzen (z. B. Online-Banking). PS: Öffentliche Ladestationen über USB statt Netzstecker sind beliebte Angriffspunkte für Hacker.

★ 09@2023

(2) Zum Datenschutz



(a) WLAN - Tracking und Datenschutz

Aus einer Artikelserie von „golem.de in aller Kürze⁶⁶:

i) WLAN & Tracking

Das Smartphone wählt sich automatisch in das private WLAN – Netzwerk ein, wenn man in Reichweite ist. Um das zu können, sendet das Smartphone regelmäßig, auch außerhalb des privaten Netzwerks, an die Umgebung ein Signal, um Zugangspunkte zu erkennen. Vielleicht will man sich ja auch in ein anderes WLAN – Netzwerk einwählen. Damit ist der „Kontakt“ ausgetauscht und dieses Smartphone kann jetzt in seiner Bewegung „getrackt“ werden (= WLAN-Tracking), ohne sich in das Netz einzuwählen. Damit kann, z. B. in Kaufhäusern, die Bewegung und die Verweildauer festgehalten und zur Optimierung des Verkaufsangebots genutzt werden.



ii) Geräte MAC - Adressen personenbezogen Daten?⁶⁷

Kurze Antwort: „Es hängt davon ab“, ob die Daten nur einen relativen Personenbezug (z.B. durch Pseudonymisierung) haben, die nur einen relativen Bezug darstellen und nur mit einer weiteren

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 19/28

Verknüpfung Personen zugeordnet werden können. Anders als bei dynamischen IP-Adressen, die vom Netzbetreiber erfasst und gespeichert werden. So das Gericht der Europäischen Union in seinem Urteil T-557/20⁶⁸ bei Weitergabe von personenbezogenen Daten im Zusammenhang mit einer Unternehmenstransaktion. Der Gerichtshof nimmt in Absätzen 92ff Bezug auf Erwägungsgrund 26 der DS-GVO

„... ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden ... ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten ...“

Die Aufsichtsbehörden in Hamburg, Bayern, Schleswig – Holstein, Baden-Württemberg und Nordrhein – Westfalen sehen den Sachverhalt etwas enger, sodass es für den Einzelfall spannend werden könnte.



iii) Wie kann man sich schützen?

Die „Tracker“ sollten sich die erhaltenen Geräte – MAC – Adressen entweder gar nicht erst speichern, oder zumindest nur für einen Aufenthalt und in jedem Fall pseudonymisieren.

Die „Getrackten“ können a) die WLAN – Funktion außerhalb gesicherter Netzwerke ausschalten, müssen diese aber bei Rückkehr wieder manuell einschalten, b) oder die Einstellung MAC – Adresse randomisieren anwenden, damit gibt das Smartphone wechselnde MAC – Adressen an. Das kann allerdings ein aktiver MAC – Adressen Filter eines Routers nicht erkennen, der aber sicherlich immer „Up to date“ ist, eine starke Verschlüsselung besitzt, mit einem starken Passwortschutz ausgestattet ist und für Dritte über einen Gastzugang verfügt.

(3) Zur Datensicherheit

(a) Basiselemente der Cyber-Sicherheit Nr. 7

i) Passwörter⁶⁹

Mit den Passwörtern ist es so eine Sache, am besten ein einfaches Passwort für alles, dann ist es aber auch einfach zu knacken und eröffnet den Kriminellen schnell „Tür und Tor“. Ein komplexes Passwort (Zeichenarten mit: „a“, „A“, „1“, „\$“ + „ä“) und für jedes Konto ein anderes, kann sich keiner mehr merken. Und dann gibt es ja noch die Konten, die in regelmäßigen Abständen ein neues Passwort erbitten. Passwort-Manager können da Abhilfe schaffen, aber sind eben auch Anwendungen, die für eine komfortable Nutzung über eine Cloud synchronisiert werden. Die Empfehlungen des BSI:

- ✓ Im Standard eingestellte Passwörter umgehend ändern.
- ✓ Für jedes Konto ein anderes Passwort
- ✓ Entweder ein kurzes, komplexes Passwort aus mindestens 8 Zeichen und vier Zeichenarten, oder ein langes Passwort mit mindestens 25 Zeichen, z. B. als ganzer Satz. Man sollte es sich gut merken können.
- ✓ Passwörter NIE an Dritte weitergeben, bzw. einsehen lassen.
- ✓ Passwortwechsel, sobald ein unsicheres Gefühl aufkommt.
- ✓ Nutzung eines Passwortmanagers, „dem man vertraut“.

ii) Zwei-Faktor Authentisierung⁷⁰

„2FA“ oder Zwei – Faktor Authentisierung kombiniert zwei unterschiedliche Zugangskanäle zur Authentisierung oder Login. Faktor 1: ist meist der klassische Zugang mit Benutzer und (starkem) Passwort. Faktor 2: ist dann z. B. eine Transaktionsnummer per SMS oder E-Mail an eine zuvor hinterlegte Mobilfunknummer bzw. Mail-Adresse. Alternativ bietet sich auch eine „Authenticator-App“ an, wie z. B. von Microsoft, Google, Apple oder eine herstellerunabhängige, wie von Sophos mit Intcept X, über ein zuvor ausgetauschtes Schlüsselpaar.



iii) Und jetzt

A. Frage: Was könnte passieren, wenn sich jemand fremdes bei dem Konto / Anbieter

anmeldet?

B. Kriterium: Je größer der mögliche Schaden, desto sicherer sollte die Authentisierung sein!

C. Entscheidung: Für sensible Konten (Firmennetzwerk, E-Mail, Applikationen mit Zahlungsfunktionen, Bank u. ä.), sollte der höchste Schutz gewählt werden! Für alle anderen Konten würde ich persönlich einen sicheren Passwortmanager bevorzugen.

(4) Zu angrenzenden Themen



(a) Alptraum für die Privatsphäre: Autos!

Die Mozilla – Foundation hat sich im Rahmen ihres Programms „Privacy not included“ die US-Datenschutzbestimmung von 25 Automobilherstellern (incl. Audi, BMW, Mercedes, VW) angeschaut⁷¹. Das Ergebnis: ziemlich erschreckend!

- ✗ Nach Herstellerangaben dürfen 84 % die Daten an Dritte weitergeben und 75 % sogar diese Daten verkaufen dürfen.
- ✗ In den Datenschutzbestimmungen finden sich auch Zustimmungen zur Sammlung von „sexueller Aktivität“, „Sexleben“, „religiöse Anschauungen“ und „genetischer Informationen“.
- ✗ Es betrifft nicht nur Fahrer und Besitzer, sondern auch Passagiere und Fußgänger in der Nähe.
- ✗ Nur bei zwei untersuchten Marken in den USA können Daten gelöscht werden, weil diese ausschließlich in der EU (DS-GVO) verkauft werden.

Als ein Beispiel einer „Leuchte im Dunkel“, auch wenn das Licht eher noch schwach ist: BMW⁷²



Zu den persönlichen Fahrdaten, Standortdaten, App- und Internetnutzung kommen noch Name, E-Mail, Telefonnummer, Adresse, Fahrzeugidentifikationsnummer (VIN), Standortdaten über Person und Auto, die Namen und Telefonnummern der Kontakte (wenn ihnen natürlich Zugang dazu geben), Fahrzeugbilder, einschließlich 3-D-Bildern rund um Ihr Auto, Umweltinformationen wie die Temperatur, wenn es sich um einen Ultraschall handelt, Gesten, Stimme usw.“, wie schnell und wo man fährt. Dazu werden Daten gesammelt aus/von Datenvermittlern, Datensammlern, Social – Media - Netzwerken, der Regierung, öffentlich zugängliche Datenbanken und mehr. Die Informationen können Kaufgewohnheiten und -interessen, andere öffentlich beobachtete Daten sowie demografische Informationen wie Alter, Geschlecht und kulturelle Identität enthalten. Das war es noch nicht, denn aus diesen Daten werden Rückschlüsse auf Vorlieben und Gewohnheiten getroffen.



Diese gesammelten Daten können innerhalb des recht großen Firmenkonglomerats von BMW und mit Drittanbietern, Dienstleistern und Geschäftspartnern geteilt werden. Wie weit diese Daten, wie bei anderen Herstellern, auch verkauft werden, ist unklar, aber der Kreis bei BMW ist so schon riesig. Für die „Leuchte im Dunkel“ finde ich es schon sehr, sehr erschreckend für die Privatsphäre!

Nach einer forsa – Umfrage im Auftrag der Verbraucherzentrale Bundesverband e.V. sehen die Deutschen das Thema „Sicherheit der Mobilitätsdaten“ mit 78 % als sehr oder eher wichtig an⁷³. Es bleibt also spannend, wie viel davon nach Europa und Deutschland „schwappt“ (oder vielleicht schon ist?).

★ 10@2023

(2) Zum Datenschutz

(a) „Best of Datenschutz“ (LfDI Rheinland-Pfalz)



Im August berichtet in einem Pressegespräch⁷⁴ die Datenschutzaufsicht in Rheinland-Pfalz über spannende (kuriose) Fälle der letzten 18 Monate, mit dem Hinweis, dass viele Menschen Wert darauf legen zu wissen, was mit Bildern und Daten von ihnen passiert.

i) Handy-Blitzer mit künstlicher Intelligenz

Die Polizei hat in Abstimmung mit der Aufsichtsbehörde ein Kamerasystem mit künstlicher Intelligenz zur Erfassung von Autofahrern/innen/* mit Nutzung eines Smartphones am Steuer getestet. Nach Abschluss konnte mit mehr als 1.000 festgestellten Verstöße und einer

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 21/28

Präventionsquote von 50 % das Projekt als deutlich erfolgreich gewertet werden. Hinweis der Aufsicht: „Jede Technologie, die zur Überwachung und Erfassung persönlicher Informationen eingesetzt wird, sollte auf einer klaren und angemessenen gesetzlichen Grundlage basieren.“ Dafür ist noch die gesetzliche Grundlage zu schaffen.

ii) Spionage durch „Nachbarkatze“

Ein Anrufer bei der Aufsicht vermutete Spionage durch die „Nachbarkatze“, die, mit einer Videokamera ausgestattet, systematisch vom Fensterbrett aus das Wohnzimmer des Anrufers ausspähe. Mit diesen Tierkameras sollen die Erlebnisse des Tieres für Halter* nachvollziehbar werden. „Für den LfDI bleiben die Erwägungen vorerst theoretisch, da der Anruf des Bürgers nicht in einer offiziellen Beschwerde gemündet ist.“ - wirklich schade – „Die Frage nach der Verantwortlichkeit im datenschutzrechtlichen Sinne ist dabei womöglich nicht trivial. Denn wie viel Einfluss hat der Halter auf das Bewegungsmuster – und damit - das vermeintliche Spionageziel – seiner Katze?“. Aber nebenbei interessant: „Nur wenig, zeigt ein Blick in die Geschichte der Spionage: Schon die CIA hat in den 1960er Jahren zu hohe Hoffnungen in die Trainierbarkeit von Katzen gesetzt. Ein makabres, millionenschweres Forschungsprojekt namens „Acoustic Kitty“ scheiterte nicht an der technischen Ausstattung des bedauernswerten Tieres mit Mikrofonen und Sendeantennen, sondern daran, dass die Katze nicht zuverlässig in Richtung der sowjetischen Botschaft laufen wollte.“



iii) „Drum prüfe, wen du beauftragst“!

Die Strom- und Gaskunden sollten schriftlich über eine Erhöhung der Preise informiert werden. Ein externer Dienstleister wurde mit der Verteilung beauftragt. 3 Monate später wurden die Briefe im Wald und in einem Keller entdeckt. Da die Umschläge alle ungeöffnet geblieben waren, wurde das Datenschutzrisiko als gering eingeschätzt. Allerdings musste der Versorger die Erhöhung zurücknehmen und die bereits vereinnahmten Beträge erstatten.

(3) Zur Datensicherheit

(a) DSGVO: Positive Konsequenzen für die IT-Sicherheit?!

It-daily.net berichtet zum 5-jährigen Jubiläum der DSGVO zu einem wichtigen „Nebeneffekt“⁷⁵.



- (a) Die meisten Datenverstöße resultieren aus IT-Vorfällen, so wurde der Schutz gegen äußere und innere Attacken massiv durch Firewalls, unerwünschten Datenverkehr mittels IDS, Datenverschlüsselung und 2-Faktor-Authentifizierung verbessert.
- (b) Um digitale Dokumente, Dateien oder Videos besser vor Angriffen durch Verschlüsselung und Erpressung, Diebstahl oder unautorisiertem Zugriff zu schützen, wurden umfangreiche Cyberresilienz (Defense-in-Depth) Strategien mit Penetrationstest und Schwachstellenprüfung entwickelt.
- (c) Eindeutige Trennung von beruflichen und privaten Daten, z. B. durch Software-Technologien wie Containerisierung bei Nutzung von privater Hardware (BYOD).
- (d) Fokussierter und nicht isolierter Blick auf das Zusammenspiel von Menschen, Prozesse und Technologien, mit besserem, gegenseitigem Verständnis und Sensibilisierung (Fachbegriffe „DevOps“ und DevSecOps“).

(b) Virtuelles Hausverbot

Die Ausführungen der Sächsischen Datenschutz- und Transparenzbeauftragten im Tätigkeitsbericht 2022 (Seite 70ff)⁷⁶ sind verständlich genug:



Privat geführte Clubs können zur Sanktionierung von Regelverstößen gegenüber Mitgliedern (virtuelle) Hausverbote verhängen und zu deren Durchsetzung personenbezogene Daten der (ehemaligen) Mitglieder, die zur Identifizierung notwendig sind, gegebenenfalls auch dauerhaft speichern.

Da ein dauerhaftes (virtuelles) Hausverbot bei groben und/oder mehrfachen Verstößen gegen die Nutzungsbedingungen ausgesprochen wird, ist auch insoweit die Verhältnismäßigkeit für eine unter Umständen dauerhafte Speicherung von Daten gegeben. Auch hat der Bundesgerichtshof (BGH) in seiner Rechtsprechung grundsätzlich keine zeitliche Begrenzung eines Hausverbots ausgesprochen, vgl. oben

genanntes BGH-Urteil.

(4) Zu angrenzenden Themen



(a) Aus Fehlern lernen: Bußgelder

i) Berlin: € 215.000⁷⁷ (sensible Daten)

Für Beschäftigte in der Probezeit wurden sensible Daten (ärztliche Behandlung, Gründung Betriebsrat u. ä.) zwecks Beurteilung der Weiterbeschäftigung tabellarisch festgehalten.

ii) Saarland: € 30.000⁷⁸ (Auskünfte)

Ein Unternehmen holte rechtsgrundlos tausende von Bonitätsauskünften ein und speicherte diese über Jahre.

iii) Niedersachsen: € 50.000⁷⁹ (Newsletter)

Betrieb eines Newsletter-Systems ohne Möglichkeit der Abmeldung.

iv) Berlin: € 300.000⁸⁰ (autom. Entscheidung)

Die Bank konnte zu abgelehnten Kreditkartenanträgen (Online) die wesentlichen Ablehnungsgründe auch gegenüber der Aufsichtsbehörde nicht nennen.

(b) Facebook Account: Feindliche Übernahme + böartige Werbung



GDATA CyberDefense berichtet auf ihrem Blog von einem konkreten Fall⁸¹: „Kriminelle kapern Business-Konten auf Facebook und schalten eigene Werbekampagnen in fremdem Namen und auf Kosten der Betroffenen. So entstehen schnell tausende Euro an Schäden für die eigentlichen Inhaber des Kontos – vom Reputationsschaden einmal ganz zu schweigen.“

Das Social – Media - Plattformen sich über Werbung finanzieren, ist kein Geheimnis. Für die Schaltung von gezielter Werbung ist die Eröffnung eines Kontos bei Facebook für Unternehmen wie Privatpersonen notwendig.

Der Köder: In einer gut aufbereiteten Direktnachricht im Namen eines renommierten Unternehmens wird eine Zusammenarbeit / Auftrag mit Budget angeboten. Zu den Details wird als Download eine ZIP - Datei aus einem gängigen oder üblichen Cloud - Speicher angeboten, die Grafiken und Office – Dateien enthält.

Gefangen: Eine, mittels Ordnersymbol versehene Datei (hier *.scr) enthält die Schadsoftware. Damit werden Session Cookies / Token mit der Zugangsberechtigung für das Konto, wie auch Screenshots gestohlen und an einen Telegram - Bot gesendet. Damit können die Täter auf das Konto zugreifen und zulasten des Kontoinhabers böartige Werbung schalten.

Schäden: Kosten für die böartigen Werbekampagnen. Nutzung des Bekanntheitsgrades, verbunden mit möglichen Reputationsschäden. Schaffen es die Täter, die Zugangsberechtigung zu ändern, ist das Konto dauerhaft verloren.

Schutz: Auch hier gilt (Empfehlungen aus dem Block):

- ✓ Nie dauerhaft angemeldet bleiben. Wenn „Browser merken“ oder „dauerhaft angemeldet bleiben“ aktiviert wurde, auf jeden Fall abmelden, dann ist auch der gestohlene Cookie / Token nicht mehr gültig.
- ✓ Zwei-Faktor-Authentisierung nutzen.
- ✓ Statt „Passwort merken“, lieber einen Passwortmanager nutzen.
- ✓ Skepsis gegenüber ungefragten und unerwarteten (Direkt-) Nachrichten.

★ 11@2023

(2) Zum Datenschutz

(a) Deal gegen Datenschutzbeschwerde?



In einem Fachbeitrag hat „Dr. Datenschutz (intersoft consulting servies)“⁸² eine rechtliche Betrachtung dazu unter Berücksichtigung eines tatsächlichen Verstoßes vorgenommen. Kurze und knappe Zusammenfassung des Ergebnisses: „Vergessen Sie das!“ Selbst wenn das Angebot der Rechte des Betroffenen mit Schadenersatz verbunden sind, lässt sich keine

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 23/28

rechtssichere Vereinbarung treffen. Zumal nicht auszuschließen und schwer nachweisbar sein wird, wenn die Beschwerde dann von einem Dritten der Aufsichtsbehörde vorgetragen wird.

Empfehlung: „Einhaltung datenschutzrechtlicher Vorgaben und die zügige Beseitigung von Datenschutzproblemen“.

(b) E-Mail Anbieterverschlüsselung (TLS) ausreichend?



Beim Versenden von E-Mails wird bei der Verschlüsselung nach Transport- und Inhaltsebene unterschieden. Jetzt wird bei der Transportverschlüsselung (TLS) jedoch nur der Weg vom Absender zu dessen Mailserver bzw. beteiligten Mailservern verschlüsselt. Auf den Mailservern liegt die Mail weiterhin im Klartext, also unverschlüsselt vor. Da der Schwerpunkt auf Zustellung und nicht auf Sicherheit liegt, kann auch das Niveau mit optionalem TLS (notfalls ohne) reduziert sein, oder es wird noch eine ältere TLS - Version eingesetzt. [Artikel 32 DS-GVO](#) schreibt ein angemessenes Schutzniveau nach dem Stand der Technik vor. Auf die Frage, ob eine TLS – Verschlüsselung ausreichend für personenbezogene Daten ist, ist jetzt vielfach zu lesen: „Kommt darauf an!“ Die Landesbeauftragte LFDI-NRW⁸³ verweist auf die Orientierungshilfe der DSK, danach gilt:

- ✓ Bei Nutzung öffentlicher Dienstanbieter hat sich der Verantwortliche zu versichern, dass ausreichende Maßnahmen zur Einhaltung der DS-GVO gegeben sind (Einhaltung der Anforderungen des BSI – TR 03108-1)
- ✓ Normales Betroffenheitsrisiko: Mindestforderndes ist der Aufbau einer gesicherten TLS – Verbindung (STARTTLS; SMTPS).
- ✓ Hohes Betroffenheitsrisiko: Neben einer qualifizierten Transportverschlüsselung ist eine End-to-End Verschlüsselung notwendig, bzw. zwingend. Ein Indiz für hohes Risiko stellt z. B. der Mailverkehr von Berufsgeheimnisträgern dar.

Zwei wesentliche Punkte aus einem Beschluss der Konferenz der Aufsichtsbehörden⁸⁴ sind:

1. „Die vom Verantwortlichen nach Art. 32 DS-GVO vorzuhaltenden technischen und organisatorischen Maßnahmen beruhen auf objektiven Rechtspflichten und stehen nicht zur Disposition der Beteiligten.“
2. „Unter Beachtung des Selbstbestimmungsrechts der betroffenen Person und der Rechte weiterer betroffener Personen kann es in zu dokumentierenden Einzelfällen möglich sein, dass der Verantwortliche auf ausdrücklichen, eigeninitiativen Wunsch der informierten betroffenen Person bestimmte, vorzuhaltende technische und organisatorische Maßnahmen ihr gegenüber in vertretbarem Umfang nicht anwendet.“

Empfehlung: Auf ein Angebot zur End-to-End Verschlüsselung von E-Mails ist nicht zu verzichten. Für einen Verzicht („nur“ TLS – Verschlüsselung) sollte in aufklärender Weise über die Risiken eine Einwilligung eingeholt werden. Bei sehr hohem Betroffenheitsrisiko ist nicht auf eine End-to-End Verschlüsselung zu verzichten!

(3) Zur Datensicherheit

(a) Warum immer wieder Microsoft?

Die Frage kann ich jetzt auch nicht wirklich beantworten, aber ein paar aktuelle Statistiken dazu:



- Marktanteile Betriebssysteme laut statista⁸⁵ im Juli 2023 Linux: 2 %, macOS X: 13 % und Microsoft: 81 %.
- Marktanteile Office-Software in Unternehmen laut statista⁸⁶ in 2020: Apple iWork, LibreOffice & Sonstige jeweils 2 %, Google Docs 9 % und MS Office 85 %.

Die Frage ist bei der aktuellen Presse schon berechtigt, warum es nicht Wanderungen zu anderen Anbietern gibt. Beispiele: Die Mozilla Foundation⁸⁷ hat 4 Juristen*, 3 Datenschutzexperten* und 2 Aktivisten* beauftragt, den Servicevertrag zu KI von Microsoft unter die Lupe zu nehmen, aber keinem Experten* gelang es eine klare Aussage zu finden. Dann war da noch die Sache mit dem

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 24/28

gestohlen Signaturschlüssel für Exchange Online⁸⁸. Laut Microsoft sei der „Fehler“ behoben, allerdings sollten man nach Expertenmeinung trotzdem auf ungewöhnliches Verhalten achten. Aber das Argument Sicherheit zieht so nicht zu 100%. Beispiel ist die Sicherheitswarnung des BSI laut news.de⁸⁹ zu SHA-3 (kryptographische Hashfunktion zum digitalen Signieren).

„Betroffen von der Sicherheitslücke sind die Betriebssysteme UNIX, Linux, MacOS X und Windows sowie die Produkte Open Source Python, Debian Linux, Amazon Linux 2, Red Hat Enterprise Linux, Open Source Ruby, Fedora Linux, Open Source PHP, Ubuntu Linux, SUSE Linux, Oracle Linux, Gentoo Linux und NetApp ActiveIQ Unified Manager.“

Und welche Einstellungen haben jetzt die Aufsichtsbehörden?

Das [Bundesamt für Sicherheit in der Informationstechnik \(BSI\)](#) stellt unter dem Suchbegriff: „Sichere Konfiguration von Microsoft“ 16 Dokumente zum Betriebssystem und einzelnen Anwendungen zur Verfügung.

Die Datenschutzaufsichtsbehörden des Bundes und der Ländern (DSK) sind da noch „gespalten“. Mit einem Paukenschlag hatten sie im November letzten Jahres Microsoft 365 als nicht DS-GVO konform bezeichnet und fühlten sich dann missverstanden. Nun ist über den Landesbeauftragten für Datenschutz Niedersachsen eine „Handreichung“⁹⁰ (Hilfe für Verantwortlich) veröffentlicht worden.

„Zudem gibt es Maßnahmen, die von den öffentlichen und nicht-öffentlichen Stellen unabhängig von vertraglichen Vereinbarungen mit Microsoft getroffen werden können, um den Datenschutz beim Einsatz von Microsoft 365 zu verbessern. Diese Maßnahmen sowie die in Betracht kommenden vertraglichen Vereinbarungen, die dazu beitragen, dass der Einsatz von Microsoft 365 datenschutzkonform erfolgen kann, sind in der folgenden Handreichung beschrieben.“

Mit anderen Worten, der datenschutzkonforme Einsatz von Microsoft 365 ist weitestgehend nicht unmöglich. Ausgenommen und noch nicht abschließend geklärt sind die Themen internationaler Datentransfer (und zu weiteren Dienstleistern) und extraterritorialer Anwendungsbereich von US – Gesetzen. Wir warten mit Spannung!

(4) Zu angrenzenden Themen

(a) *Mein Smartphone belauscht mich (?)*

„Der Standard“ klärt in der Rubrik „Web-Netzpolitik“⁹¹ sehr ausführlich und in vielen Punkten für jeden nachvollziehbar darüber auf, was die großen „Plattformen“ können bzw. nicht können:

Um es kurz zu machen: Nein, kann es nicht. Es handelt sich hierbei um eine besonders hartnäckige Verschwörungstheorie, die mittlerweile seit fast einem Jahrzehnt durchs Netz geistert.

i) Die Verschwörungstheorie

Technisch wäre es nur für Meta & Co. eine unbeherrschbare und kostenintensive Menge an Daten und Serverkapazitäten (20 Petabyte pro Tag nur für die USA, Meta) und die Akkulaufzeit würde sich dramatisch verkürzen. Auch eine lokale Spracherkennung würde den Ressourcenverbrauch dramatisch erhöhen. Zumal die Betriebssysteme so weit optimiert sind, dass eine Mikrofonnutzung erst genehmigt werden muss und diese bei aktiver Nutzung angezeigt wird. Die Sprachassistenten reagieren (Aktivierung) erst auf bestimmte Begriffe (Hey Google, Siri, Alexa), bzw. deren Klang. Bei ähnlichen Sprach- und Wortklängen erfolgt eine versehentliche Aktivierung.

ii) Was ist es dann?

Zunächst mal „der rosarote Elefant“, d. h. vielleicht wird die Werbung regelmäßig angezeigt, jedoch erst, wenn wir darüber gesprochen haben, wird uns diese Werbung bewusst, bzw. fällt uns auf. Dazu kommt Werbung, die durch Thementrends (häufige Suche, Blogs u.) ausgelöst wird. Ein großer Lieferant sind wir selber durch die Nutzung (was, wie lange, wo usw.). Laut Artikel hat zum Beispiel Facebook 52.000 unterschiedliche Attribute für seine User*innen*. Da diese Firmen oft auch unsere Freunde und Freundesfreunde*innen* kennen (Adressbuch) lassen sich durch „Den Algorithmus“ (stark vereinfacht) die Interessen sehr gut in Thema und Zeit eingrenzen.

★ 12@2023

(2) Zum Datenschutz

(a) *Öffentlich zugängliche Daten verarbeiten*⁹²

Dokument von <https://volkerschroer.de/DSGVO/Datenschutz.html>

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 25/28

Wie verhält es sich jetzt mit der Verarbeitung von Daten, die von Personen selbst öffentlich gemacht oder gegeben werden, z. B. Telefonbuch, Visitenkarte, Webseiten u. ä.?

i) **Nach den Vorschriften:**

Nach [Art.1 der DS-GVO](#) dient die Vorschrift dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und deren personenbezogener Daten bei der Verarbeitung und dem freien Verkehr solche Daten.

„Keine Verarbeitung ohne Rechtsgrundlage!“ [Art.6 DS-GVO](#). Als Rechtsgrundlage bleibt nach Art.6 Abs.1 nur f), das berechtigte Interesse des Verantwortlichen oder eines Dritten, sofern die Interessen der Person nicht überwiegen. Dazu wird in den [Erwägungsgründen unter \(47\)](#) ausgeführt:

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

Vorsicht ist in Bezug auf [§7 UWG](#) gegeben, da belästigende Werbung in unzumutbarer Weise verboten ist. Bei Werbemaßnahmen sollte m. E. immer eine Einwilligung eingeholt werden.

Nach [Art.9 Abs.1 GS-GVO](#) gilt auch für diese Daten das Verarbeitungsverbot mit Erlaubnisvorbehalt. Allerdings gilt nach Art.9 Abs.2 e) dies nicht für die Verarbeitung von personenbezogenen Daten, die die betroffene Person offensichtlich öffentlich gemacht hat. Dafür besteht aber die Pflicht nach [Art. 14 DS-GVO](#) zur Information, wenn die Daten nicht direkt beim Betroffenen erhoben werden.

ii) **Kurz zusammengefasst:**

- ▶ Visitenkarten u. ä. werden i. d. R. direkt beim Betroffenen erhoben und es kann eine Genehmigung zur Verarbeitung zu Kontaktzwecken unterstellt werden.
- ▶ Bei Datenerhebung von dritter Seite (z. B. Telefonbuch, Webseite) ist – immer – der/die Betroffene in transparenter Form nach den Vorschriften des Art.14 DS-GVO zu informieren.
- ▶ Für Werbemaßnahmen besser immer eine direkte Einwilligung einholen.
- ▶ Verarbeitung von öffentlich zugänglicher Daten bedürfen immer einer Abwägung der Interessen des Verantwortlichen und des Betroffenen. Dies sollte mindestens im Verzeichnis der Verarbeitungstätigkeiten Erwähnung finden und dokumentiert sein.

(b) **Das Smartphone als DS-GVO Falle**

Datenschutz und Smartphone empfinde ich als ein recht heikles Thema. Wir sind „Mobil“ unterwegs und in vielen Fällen auch erreichbar. Überspitzt formuliert, vermischen sich leicht private und geschäftliche Kontaktdaten auf unseren Smartphones. Als Datenschutzbeauftragter fangen die Fragen schon bei den Betriebssystemen von Apple, Google und Microsoft an (oder vielleicht schon bei den Herstellern) und hören bei den Apps nicht auf. Mal ein kleiner

i) **Kurzcheck:**

Prüfung der Zugriffskontrolle bei einem Google / Android Smartphone auf die Kontakte über >Einstellungen >Datenschutz >Privatsphäredashboard >Kontakte. Dort werden die Dienste (Apps) angezeigt, die zugriffsberechtigt sind und wann der letzte Zugriff auf das Adressbuch erfolgte. Unter >Anruflisten (statt Kontakte die gleichen Anzeigen).

PS: Bei separater Speicherung in einer Anwendung (Programm u/o App) ohne Zugriffsberechtigung zum Adressbuch, ist bestimmt ein Blick auf die Datenschutzbestimmungen gefallen.

ii) **Die Datenschutzfrage!**

Ist der Kunde (der Betroffene) vollumfänglich und leicht verständlich über Art, Zweck, Dauer und Verarbeitung seiner erhobenen Daten informiert und hat genau dazu sein Einverständnis gegeben?

PS: Für alle Adressbucheinträge würde ich bei Meta/Facebook, X, Instagram u. ä. meine Zweifel hegen.

iii) **Ausnahme(n)?**

Übersicht 2023 | Zum Datenschutz aufgefallen Seite 26/28

Selbst die Haushaltsausnahme ([Art.2 c DS-GVO](#)) zu persönlicher, familiärer Verarbeitung kennt Grenzen. Frage: „Besteht zu jedem Adressdatensatz eine persönliche, familiäre Grundlage, bzw. liegt eine Einwilligung vor und werden die Daten DS-GVO konform verarbeitet?“ Darunter fallen bestimmt keine Social-Media-Plattformen u. ä.

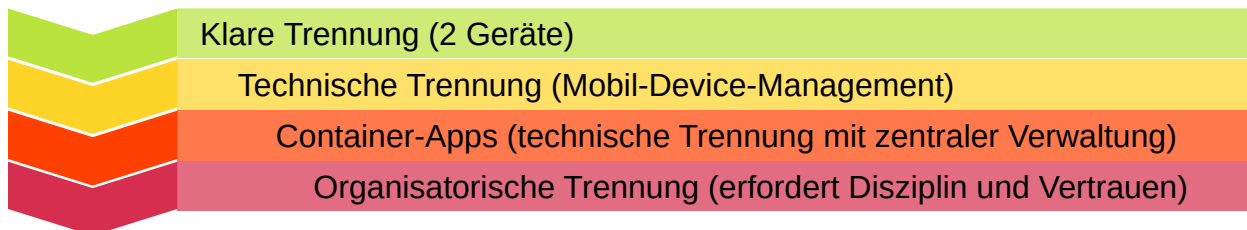
iv) **Datenschutzrisiken**

Für mich nicht abschließend, aber gut sind die Ausführung unter [wirtschaftswissen.de](#) zu „Datenschutz bei betrieblich genutzten Handys“⁹³. Ob Firmen- oder Privathandy, Risiken bestehen für beide Seiten. Ausschnitte aus den Ausführungen:

Für das Unternehmen ergeben sich aus der betrieblichen Nutzung des Handys zahlreiche Probleme. In der Regel kann das Unternehmen weder die Sicherheitsanforderungen der Datenschutzgesetze gewährleisten, noch die Rechte der betroffenen Personen erfüllen oder eine rechtmäßige Datenübermittlung in Drittländer sicherstellen. In den meisten Fällen fehlen auch die erforderliche Rechtsgrundlage und die Möglichkeit zur Datenlöschung nach Erreichen des Zwecks.

..... Die Verwendung vertraulicher Daten auf dem privaten Gerät, für die möglicherweise eine Verschwiegenheitsvereinbarung besteht, kann ebenfalls erhebliche Konsequenzen nach sich ziehen.

Der Einsatz eines privaten Geräts für dienstliche Zwecke mag gut gemeint sein, führt in der Regel aber zu Verstößen gegen die Unternehmensrichtlinien (Wahrung der Vertraulichkeit). Diese Verpflichtung umfasst normalerweise die Verarbeitung personenbezogener Daten, die nur auf vorgesehenen Geräten und in genehmigten Anwendungen durchgeführt werden dürfen. Da private Geräte, Anwendungen (Apps) und Dienste wie Google-Kalender oder iCloud in der Regel weder vorgesehen noch genehmigt sind, stellt die Nutzung einen Verstoß gegen die Vorgaben des Arbeitgebers dar. Darüber hinaus besteht die Möglichkeit, dass der Mitarbeiter als Verantwortlicher im Sinne der Datenschutzgesetze gilt und somit die gesetzlichen Anforderungen erfüllen muss.



(3) **Zur Datensicherheit**

(a) **Tipps Datensicherheit Smartphone**

Aus dem bereits in der Fußnote verlinkten Artikel noch ein paar Tipps zu Datensicherheit bei Mobilgeräten.

- ✓ Nach Möglichkeit die Verwendung von sicheren Passwörtern, Authentifizierung mit Fingerabdruck u/o Gesichtserkennung und bei bedeutenden Anwendungen möglichst eine 2-Faktor-Authentifizierung.
- ✓ Bei immer aktuellen Stand der Software, Aktivierung der Geräteverschlüsselung (meist Standard) und die Verschlüsselung vertraulicher Kommunikation. Vorsicht besteht bei Anwendungen aus nicht nachweislich vertrauenswürdigen Quellen, öffentlichen WLANs sowie öffentlichen USB-Ladestationen.
- ✓ Niemals das Gerät in unbeobachtete Hände geben.

(4) **Zu angrenzenden Themen**

(a) **Microsoft PC Manager**

Wer sein Windows-System aufräumen möchte, kann auf eine Vielzahl praktischer Werkzeuge zurückgreifen. Die Kernfunktionen sind – egal ob kostenlos oder kostenpflichtig – recht ähnlich. Microsoft hat jetzt eine eigene Anwendung entwickelt, aber noch nicht beworben. Nach meinem ersten Eindruck „nicht schlecht“, die Qualität zeigt sich wohl erst mit der Zeit⁹⁴.

Bei Bedarf, einfach mal sprechen!



- 1 Quelle: FAZ Datenschutz: „EU erleichtert Datentransfer in die USA“
- 2 Quelle: BSI „DIGITALBAROMETER. Bürgerbefragung zur Cyber-Sicherheit-2022“
- 3 Quelle: t3n „FBI empfiehlt Werbeblocker gegen Cyberkriminalität“
- 4 Quelle: heise online „NortonLifeLock: Hersteller warnt vor potenziell geknackten Passwortmanagern“
- 5 Quelle: heise online: „Passwortmanager LastPass: Hacker haben Zugriff auf Kennworttresore von Kunden“
- 6 Quelle: GIGA: „Samsung wichtiges Dezember Update!“
- 7 Quelle: heise online: „Netgear schließt hochriskante Lücke in mehreren Routern.“
- 8 Quelle: heise online: „Tausende Citrix-Sever sind noch verwundbar.“
- 9 Quelle: <https://dejure.org/gesetze/UWG/7.html>
- 10 Quelle: Einwilligung: DS-GVO Art.4 Nr.11 <https://dejure.org/gesetze/DSGVO/4.html>
- 11 Quelle: Informationspflichten: DS-GVO Art.13, 14, 15 <https://dejure.org/gesetze/DSGVO/13.html>
- 12 Quelle: LfDI – Baden-Württemberg: „Einbindung von Videos in eigene Webseiten“
- 13 Link: PeerTube-Instanz: <https://joinpeertube.org/instances>
- 14 Quelle: [tagesschau>faktfinder>peertube](#)
- 15 Quelle: Jahresübersicht Datenschutzinfo 2021: „Was ist jetzt mit Fotos“, Seite 16
- 16 Quelle: Jahresübersicht Datenschutzinfo 2022: „Mitarbeiter Information & Einwilligung(en)“, Seite 6
- 17 Quelle: chip.de: „Betrieb auf eigenes Risiko: Welchen FritzBoxen Sie den Stecker ziehen sollten“
- 18 Quelle: Mozilla: „See No Evil: Loopholes in Google's Data Safety Labels Keep Companies clear and Consumer in the Dark“
- 19 Quelle: Mozilla: „Datenschutz nicht inbegriffen (Aufstellung analysierter Apps)“
- 20 Quelle: fintus: „ChatGPT in Verbindung mit #lowcode – der Gamechanger in der Kreditrisikoprüfung?“
- 21 Quelle: t-online: „Du liebst sie nicht“: Plötzlich zeigt der Chatbot seine dunkle Seite“
- 22 Quelle: chip.de: „Fehler in ChatGPT, Bing & Co.: Wie Sie KI-Tools besser nutzen und wo Grenzen sind“
- 23 Quelle: DS-GVO – Portal: „BREBAU GmbH / LfDI-Bremen“
- 24 Quelle: DS-GVO – Portal: VW / LfDI-Niedersachsen“
- 25 Quelle: DS-GVO – Portal: Hannoversche Volksbank / LfDI-Niedersachsen“
- 26 Quellen: DS-GVO – Portal: „E-Commerce“; „Gesundheitswesen“; „Bauunternehmen“
- 27 Quelle: LfDI – NRW: „Verbindliche interne Datenschutzvorschriften (BCR)“
- 28 Quelle: BSI: „DNSSEC – Tauglichkeit von Internetzugangsroutern“ (PDF)
- 29 Quelle: IRights Info: „Tagesschau und Kolleg24 veröffentlichen Erklärvideos unter CC BY-SA“
- 30 Quelle: [cc creative commons License Chooser](#)“
- 31 Quelle: faz.net: „Mehr Transparenz oder mehr Datenschutz? Gutachten deutschen Familienunternehmer fordert letzteres.“
- 32 Quelle: HambBfDI: „Pressemitteilung zur Veröffentlichung des Tätigkeitsbericht 2022“
- 33 Quelle: BayLDA Auslegungshilfe: „Steuerberater* - keine Auftragsverarbeiter (PDF)“
- 34 Link: PC-Welt: „Die beste Backup-Software für Windows im Test (2023)“
- 35 Link: BSI-Newsletter: „BCM, Cloud-Computing, IT-Grundschutz, KMU, Verbraucherschutz“
- 36 Quelle: EUR-Lex: „Richtlinie (EU 2019/1937) des EU-Parlaments und des Rates vom 23. Oktober 2019“
- 37 Quelle: Bundesministerium der Justiz: „Gesetz für einen besseren Schutz hinweisgebender Personen ...“
- 38 Quelle: Bundesregierung: „Besserer Rechtsschutz für „Whistleblower“
- 39 Quelle: DSK: „Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines“ (PDF)
- 40 Hinweis: V. Schroer: „Zusammenfassende Erläuterung zum Verzeichnis der Verarbeitungstätigkeiten“
- 41 Hinweis: V. Schroer: „Zusammenfassung Das Standard - Datenschutz - Modell | Management – Info“
- 42 Quelle: AV Test GmbH: „Testübersichten“, für „Privatanwender“, für „Unternehmen“
- 43 LINK: [VIRUSTOTAL](#)
- 44 Quelle: European Data Protection Board: „Leitlinie 3/2019 zur Verarbeitung pb Daten durch Videogeräte“
- 45 Quelle: Datenschutzkonferenz: „Kurpapier Nr. 15 Videoüberwachung nach der Datenschutz-Grundverordnung“
- 46 Quelle: haufe.de: „Was bei der Mitarbeiterüberwachung erlaubt ist“
- 47 Quelle: BSI: „Basiselemente der Cyber-Sicherheit“
- 48 Quelle: Wikipedia: „Firewall“
- 49 Quelle: Microsoft / Learn / Sicherheit: „Bewährte Methoden zum Konfigurieren von Windows Defender Firewall“
- 50 Quelle: Chip.de: „Free Firewall“
- 51 Quelle: Vergleich.org: „Firewall Vergleich 2023“
- 52 Quelle: BSI: „Basis IT-Sicherheit Firewall“; „Baustein NET.3.2: Firewall (Edition 2021)“
- 53 Quelle: tagesschau.de: „EU und USA Neues Datenschutzabkommen in Kraft“
- 54 Quelle: noyb.eu: „Europäische Kommission gibt EU-US Datentransfers 3. Runde beim EuGH“
- 55 Quelle: Internet World: „Das EU-US-Datenschutzabkommen ist völlig wertlos, ein Fiasko für die Wirtschaft“
- 56 Quelle: BfDI Pressemitteilung: „Angemessenheitsbeschluss zum EU-U.S. Data Privacy Framework in Kraft getreten“
- 57 Quelle: eset: „Threat Report H1 2023 December 2022 – May 2023 (PDF)“
- 58 Quelle: BSI: „Empfehlungen: IT in Unternehmen. Sichere Konfiguration von MS Office...“
- 59 Quelle: tagesschau.de: „EU-„Data Act“ neue Regeln zur Daten-Weitergabe von Geräten“
- Quelle: EUR-Lex: „DOK 52022PC0068 EU-Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz)“
- 60 Quelle: Oberlandesgericht Hamm, 8 U 94/22: „Vereinsmitglied, Mitgliederliste, E-Mail-Adressen, Datenschutz“
- 61 Quelle: Blog CMS Deutschland: „Data Ownership – Keine Eigentumsrechte an Daten“
- 62 Quelle: Smart-Data-Begleitforschung FZI Berlin: „Daten als Wirtschaftsgut“ (PDF)
- 63 Quelle: BSI „Spam-Phishing & Co. So erkennen Sie gefälschte und schadhafte E-Mails“
- 64 Quelle: Allianz-für-Cybersicherheit: „Awareness-Poster „Psychotricks und Phishing-Maschen“
- 65 Link: chip.de: „Anleitung für die Ersteinrichtung im Praxistipp > Android von chip.de.“
- 66 Quelle: golem.de: „Ist das Tracken von Nutzen übers Smartphone legal?“
- 67 Quelle: golem.de: „Die rechtliche Situation ist kompliziert“
- 68 Quelle: EuG: „In Rechtssache T-557/20“
- 69 Quelle: BSI – DINA4 Merkblatt: „BSI - Basisschutz: Sichere Passwörter (PDF)“
- 70 Quelle: BSI: „Zwei-Faktor-Authentisierung. Mehr Sicherheit für Online-Konten und vernetzte Geräte“

- 71 Quelle: Mozilla Foundation: „[Privacy not included – Cars](#)“
- 72 Quelle: Mozilla Foundation „[Privacy not included – Cars/BMW](#)“
- 73 Quelle: Verbraucherzentrale Bundesverband e.V.: „[Vernetztes Auto: Wer Daten will, muss Sicherheit bieten](#)“
- 74 Quelle: LfDI-RP [Pressegespräch „Best of Datenschutz – Spannende Datenschutzfälle aus 2022 und 2023“](#)
- 75 Quelle: it-daily.net: „[Die DSGVO und ihre positiven Konsequenzen für die IT-Sicherheit](#)“
- 76 Quelle: „[Tätigkeitsbericht Datenschutz 2022 der Sächsischen Datenschutz- und Transparenzbeauftragten 2022 \(S.70ff\)](#)“
- 77 Quelle: DSGVO-Portal: „[dsgvo-bussgeld-gegen-humboldt-forum-2023-08-02](#)“
- 78 Quelle: DSGVO-Portal: „[dsgvo-bussgeld-gegen-unternehmen-2023-06-21](#)“
- 79 Quelle: DSGVO-Portal: „[dsgvo-bussgeld-gegen-versandhändler-2023-06-15](#)“
- 80 Quelle: DSGVO-Portal: „[dsgvo-bussgeld-gegen-berliner-bank-2023-05-31](#)“
- 81 Quelle: GDATA: „[Feindliche Account-Übernahme: Böartige Werbung via Facebook](#)“
- 82 Quelle: Dr. Datenschutz: „[Datenschutzbeschwerde per Deal vermeiden](#)“
- 83 LfDI-NRW: „[Technische Anforderungen an technische und organisatorische Maßnahmen beim E-Mail-Versand](#)“
- 84 DSK: „[Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen ... auf ausdrücklichen Wunsch](#)“
- 85 Statista: „[Marktanteile der führenden Betriebssysteme in Deutschland von Januar 2009 bis September 2023](#)“
- 86 Statista: „[Meistgenutzte Office-Software von Büromitarbeitern in Unternehmen in Deutschland im Jahr 2020](#)“
- 87 Mozilla Foundation: „[Fragen Sie Microsoft: Trainiert ihr eure KI mit unseren persönlichen Daten?](#)“
- 88 Deutschland sicher im Netz: „[Schwachstelle bei Microsoft - 60.000 Regierungsmails gestohlen](#)“
- 89 Quelle: news.de: „[SHA-3 Implementierungen: Update für IT-Sicherheitswarnung \(Risiko: hoch\)](#)“
- 90 Quelle: LfD-Niedersachsen: „[Einsatz von Microsoft 365: Praxis-Tipps für Verträge mit Microsoft](#)“
- 91 Quelle: Der Standard: „[Belauschen Instagram, Facebook oder gar das ganze Smartphone Gespräche?](#)“
- 92 Quelle: Dr. Datenschutz: „[Die Verarbeitung von öffentlich zugänglichen Daten](#)“
- 93 Quelle: wirtschaftswissen.de: „[Datenschutz bei betrieblich genutzten Handys](#)“
- 94 Quelle: Microsoft: „[Safeguard your PC in a quiet and reliable way](#)“