



Liebe(r) Leser(in),\*

## Datenschutz → einfach praktisch hilfreich!

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

Mein Ziel ist es, den Datenschutz einfach, praktisch und hilfreich zu vermitteln und zu gestalten. Von Datenschutzberater, Datenschutzberatung, 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](mailto:Mail2@volkerschroer.de)

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

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

## Inhalt

(Einfach interessantes Thema nach Wahl anklicken)

1. Standard – Datenschutz – Modell Vers. 3.0.....1	ii) VW € 1,1 Mio.....2	(a) DNS – sicherer Zugriff auf das Internet-Telefonbuch...2
Letzte Ergänzung: 12/2022: SDM Version 3.0.....1	iii) Hannoversche Volksbank: € 0,9 Mio.....2	i) Ein Anbietertest:.....3
2. Zum Datenschutz.....1	iv) Weiteres Fehlverhalten...2	ii) Fazit:.....3
(a) Aus Fehlern lernen.....1	(b) Datenschutz in Gruppenunternehmen / Konzernen.....2	iii) Hinweis:.....3
i) BREBAU GMBH € 1.9 Mio. ....2	3. Zur Datensicherheit.....2	4. Zu angrenzenden Themen....3
		(a) Was bedeutet dieses „CC-BY-SA“?.....3

## 1. Standard – Datenschutz – Modell Vers. 3.0



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

	<a href="#">Zusammenfassung SDM (11 Seiten)</a>		<a href="#">Link DS - GVO auf dejure.org</a>
	<a href="#">Link zum SDM der Aufsicht (77 Seiten)</a>		<a href="#">Link BDSG auf dejure.org</a>

### Letzte Ergänzung: 12/2022: SDM Version 3.0

Mit den 6 weiteren Seiten wird im Wesentlichen die Prüfroutine für eine Datenschutzprüfung anschaulicher und detaillierter erläutert. Was ich auf den zweiten Blick durchaus nachvollziehen konnte. 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).

## 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.<sup>1</sup>**

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.<sup>2</sup>**

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

**iii) Hannoversche Volksbank: € 0,9 Mio.<sup>3</sup>**

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 Werbeprojekte zu erstellen.

**iv) Weiteres Fehlverhalten<sup>4</sup>**

**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.



Die Landesbeauftragte für den Datenschutz und die Informationsfreiheit NRW hat dazu einige Erstinformationen veröffentlicht<sup>5</sup> 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**

Das 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

1 Quelle: [DS-GVO – Portal: „BREBAU GmbH / LfDI-Bremen“](#)

2 Quelle: [DS-GVO – Portal: VW / LfDI-Niedersachsen](#)

3 Quelle: [DS-GVO – Portal: Hannoversche Volksbank / LfDI-Niedersachsen](#)

4 Quellen: [DS-GVO - Portal: „E-Commerce“](#); [„Gesundheitswesen“](#); [„Bauunternehmen“](#)

5 Quelle. LfDI – NRW: [„Verbindliche interne Datenschutzvorschriften \(BCR\)“](#)

„Namensadresse“ ([www.volkerschroer.de](http://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 Internetzugangsroutern<sup>6</sup>:



*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 umzustellen<sup>7</sup>. 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 Urheberrechtlizenzen 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 Verwendung minimieren will. Einen Lizenztyp mit Symbolen, Text und Links zur eigenen Verwendung lässt sich leicht für alle Gelegenheiten zusammenstellen<sup>8</sup>.

Bei Bedarf, einfach mal sprechen!

<sup>6</sup> Quelle: BSI: „DNSSEC – Tauglichkeit von Internetzugangsroutern“ (PDF)

<sup>7</sup> Quelle: IRights Info: „Tagesschau und Kolleg24 veröffentlichen Erklärvideos unter CC BY-SA“

<sup>8</sup> Quelle: „cc creative commons License Chooser“