Einleitung:

Ein schlankes Verzeichnis der Verarbeitungstätigkeiten (VVT) nach den Vorschriften der DS-GVO Erwägungsgrund (82)[1], Art.30[1] und des BDSG §70[1] und Anregungen aus dem Kurzpapier Nr.8[1] der Datenschutzkonferenz. Das Gute, es gibt ein Muster der Aufsicht, aber keine Formvorschrift. (!!!)

Auch wenn wir mal voraussetzen, dass nach §38 Abs.1 BDSG keine Datenschutzbeauftragter zu bestellen ist, weil weniger als 20 Mitarbeiter (vielleicht bald 50 Mitarbeiter) mit der Verarbeitung beschäftigt sind, keine geschäftsmäßige Datenübermittlung oder Sammlung zu Markt- und Meinungsforschung erfolgt und kein hohes Risiko für die Betroffenen besteht. Wenn doch, ist es eine gute Vorbereitung.

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

„Wird sehr selten vorkommen!“.

In einfachen Schritten zur Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten

Inhaltsverzeichnis

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

1. Musteransicht **2**

2. Die wichtigtsten Anforderungen **3**

i. Grundsätzliches (ErwG 82 DS-GVO) *3*
ii. Form, Inhalt, Hinweise (Art.30 DS-GVO) *3*
iii. Und (BDSG §70) *3*
iv. Sinnvolle Ergänzungen und Anmerkungen *3*

3. Die einfachen Schritte zum Verzeichnis der Verarbeitungstätigkeiten **4**

(a) Schritt 1 (Sammeln/Speichern) 4
(b) Schritt 2 (Verwendung, Verknüpfung, Weitergabe) 4
(c) Schritt 3 (Einschränkung, Löschung) 4
(d) Schritt 4 (Rechtsgrundlage & Information) 5
(e) Schritt 5 (Datensicherheit) 5
(f) Schritt 6 (Ergänzen und zusammenführen) 5

4. FAQ – oft gestellt Fragen: **6**

i. Verarbeitung öffentlich zugänglichen Daten *6*
ii. Austausch Kontaktdaten (u.a. Visitenkarten) *6*
iii. Datensicherheit zum Datenschutz *6*
iv. Geeignete technische Maßnahmen zur Datensicherheit? *7*
v. Falscher Empfänger personenbezogener Daten *8*
vi. Die Sache mit dem „berechtigten Interesse“ *9*
vii. „Haushaltsausnahme“, was ist PRIVAT? *10*
viii. E-Mail Marketing (da war was) *11*
ix. E-Mail Anbieterverschlüsselung (TLS) ausreichend? *12*
x. Videos auf der eigenen Website einbinden *13*

1 *Quellen: Erwägungsgrund (82) | DS-GVO Art.30 | BDSG §70 | DSK Kurzpapier Nr. 8*

CC BY SA

1. Musteransicht

Verzeichnis der Verarbeitungstätigkeiten

Aktuelle Version: [Nr. der Version] Datum: [Datum der Version]

Vorversion: [Nr. der Vorversion] Datum: [Datum der Vorversion]

Erstellt von/mit:

Zur Organisation

[Rechtliche Bezeichnung, Namen der Verantwortliche & Funktionen, ggf. Datenschutzbeauftragter, Vertreter und alle Kontaktdaten]

[Gegestand und Zweck der Organisation]

A.) Datenerhebung, -aufbereitung, -speicherung

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

B.) Datenverwendung, -verknüpfung, -weitergabe

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

C.) Datenverwendung Einschränkung und Löschung

Zu lfd. Nr. A	Aktivität Daten	Anwendung Applikation	Infrastruktur
1	<Bei Widerruf, Abbestellung>	<Mailsoftware>	<PC, Mailservice>
2	<Einschränkung bei Vertrags-ende, Löschung nach GoBD>	<Office-Suite, Abrechnungs-software, Buchhaltung>	<PC, Mailservice>

D.) Rechtsmäßigkeit der Verarbeitung

Zu lfd. Nr. A	a) Einwilligung zur Verarbeit-ung	b) Vertragser-füllung oder die Anbahnung*	c) Rechtliche Verpflichtung	d) Wichtige Interessen der Betroffenen	e) Im öffent-lichen Interesse vorgeschrieben	f) Berechtigtes Interesse Ver-antwortliche
1	X, bestätigt.					
2		X1	X2 nach GoBD			

E.) Sicherung der Verfügbarkeit, Vertraulichkeit und Integrität

je-weils	O = organisatorische Maßnahmen | T = technische Maßnahmen | I = Betroffene informiert
T.)	<Zentral gesteuerte Firewall und Virenscanner>
O.)	<Unternehmensweite Mitarbeiterrichtlinie zum Datenschutz und Datensicherheit>

CC BY SA

2. Die wichtigtsten Anforderungen

Es ergeben sich Anforderungen an die Form (F, 1x), den Inhalt (I, 6x) und Hinweise (H)

i. Grundsätzliches (ErwG 82 DS-GVO)

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

ii. Form, Inhalt, Hinweise (Art.30 DS-GVO)

Der Artikel regelt die erforderlichen Angaben zum „Verzeichnis der Verarbeitungstätigkeiten:

(F) Dokumentation in schriftlichem oder auch in elektronischem unterzeichnetem Format (Abs.3).

(I1) Name und Kontaktdaten von Verantwortlichen und ggf. Datenschutzbeauftragen (Abs.1a).

(I2) Beschreibung von Zweck und Kategorien der Personen & Daten der Verarbeitung (Abs.1b,c).

(I3) Wer erhält Daten (interne & externe Empfänger in Europa, Drittland, intern. Organisation)

(I4) und ist die Einhaltung der Datenschutzvorschriften (ex EU) gewährleistet. (Abs.1d,e i.V.m.Art.49).

(H) Wenn möglich, vorgesehene Löschfristen und eine allgemeine Beschreibung der technisch – organisatorischen Schutzmaßnahmen nach Verhältnismäßigkeit und dem aktuellen Stand der Technik (Abs.1f,g i.V.m. Art.32).

(H) Die gleichen Angaben sind für Auftragsverarbeiter (Dienstleister) zu dokumentieren (Abs.2).

iii. Und (BDSG §70)

Zu den Regeln der DS-GVO sind nach dem Bundesdatenschutzgesetz § 70 zu ergänzen:

(I5) Rechtsgrundlage der Verarbeitung (Abs.1 Nr.7).

(I6) Alternativ zu Löschfristen die Überprüfungstermine zur Notwendigkeit (Abs. 1 Nr.8).

iv. Sinnvolle Ergänzungen und Anmerkungen

(a) Zum Nachweis der technisch-organisatorischen Maßnahmen dienen:

- ★Datum der Erstellung und letzte Änderung,
- ★Art und Transparenz der Einwilligung,
- ★Aufstellung der Auftragsverarbeiter,
- ★Sensibilisierungsmaßnahmen der Mitarbeiter
- ★Einhaltung der Betroffenenrechte (Info, Auskunft, Löschung, Berichtigung u.ä.)
- ★Umgang mit Meldepflichten, Schutzverletzungen und Risikoeinschätzungen.

(b) Formfreiheit

Ob die Dokumentation auf Papier, in einer Tabelle, Textdatei oder in einer Anwendung erfolgt, ist eine Frage der Notwendigkeit und Effizienz (Tool, App ist reine Frage der Quantität).

(c) Arbeit mit Anlagen

Für die Schutzmaßnahmen erstellt der IT-Dienstleister i. d. R. ein Sicherheitskonzept. IT-Dienstleister, Softwareanbieter, Steuerberater, Telekommunikation und alle anderen Dritten als Auftragsverarbeiter (sollten und müssten) ihre DS-GVO Konformität und Unterstützung bestätigen.

(d) Berechtigungen

Zu ergänzen sind nur noch die eigenen Maßnahmen (Zugriffsschutz), die auch als separate Anlage beigefügt werden können.

CC BY SA

3. Die einfachen Schritte zum Verzeichnis der Verarbeitungstätigkeiten

Die Schritte sind nach und nach auszuführen, um am Schluss ein einfaches Verzeichnis erstellen zu können. Im weiteren Verlauf sind auch einige Hinweise (FAQ) zu den Themen angefügt.

(a) Schritt 1 (Sammeln/Speichern)

Welche Daten werden mit welcher Anwendung auf welcher Infrastruktur erhoben?

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

Einfach in Tabelle- oder Textdokument kopieren und sammeln, danach zu Schritt 2.

(b) Schritt 2 (Verwendung, Verknüpfung, Weitergabe)

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

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

Einfach in Tabelle- oder Textdokument kopieren und sammeln, danach zu Schritt 3.

(c) Schritt 3 (Einschränkung, Löschung)

Wird die Datennutzung nach dem Zweck eingeschränkt und gelöscht?

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

Einfach in Tabelle- oder Textdokument kopieren und sammeln, danach zu Schritt 4.

CC BY SA

(d) Schritt 4 (Rechtsgrundlage & Information)

Ist nach Art.6 DSGVO eine der folgenden Bedingungen für die Verarbeitung erfüllt?

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

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

Einfach in Tabelle- oder Textdokument kopieren und sammeln, danach zu Schritt 5.

(e) Schritt 5 (Datensicherheit)

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

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

Einfach in Tabelle- oder Textdokument kopieren und sammeln und zu Schritt 6

(f) Schritt 6 (Ergänzen und zusammenführen)

Verzeichnis der Verarbeitungstätigkeiten

Aktuelle Version: [Nr. der Version] Datum: [Datum der Version]

Vorversion: [Nr. der Vorversion] Datum: [Datum der Vorversion]

Erstellt von/mit:

Zur Organisation

[Rechtliche Bezeichnung, Namen der Verantwortliche & Funktionen, ggf. Datenschutzbeauftragter, Vertreter und alle Kontaktdaten]

[Gegestand und Zweck der Organisation]

Einfach in Tabelle- oder Textdokument kopieren und die Schritte 1 bis 5 anfügen, signieren und … fertig.

CC BY SA

4. FAQ – oft gestellt Fragen:

i. Verarbeitung öffentlich zugänglichen Daten

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

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

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

Dokumentieren bitte nicht vergessen!

ii. Austausch Kontaktdaten (u.a. Visitenkarten)

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

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

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

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

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

iii. Datensicherheit zum Datenschutz

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

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

- Die Technik sollte schon dem aktuellen Niveau entsprechen.

„… der Implementierungskosten“

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

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

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

CC BY SA

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

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

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

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

iv. Geeignete technische Maßnahmen zur Datensicherheit?

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

(a) Leichter Einstieg (KMUs)[2]

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

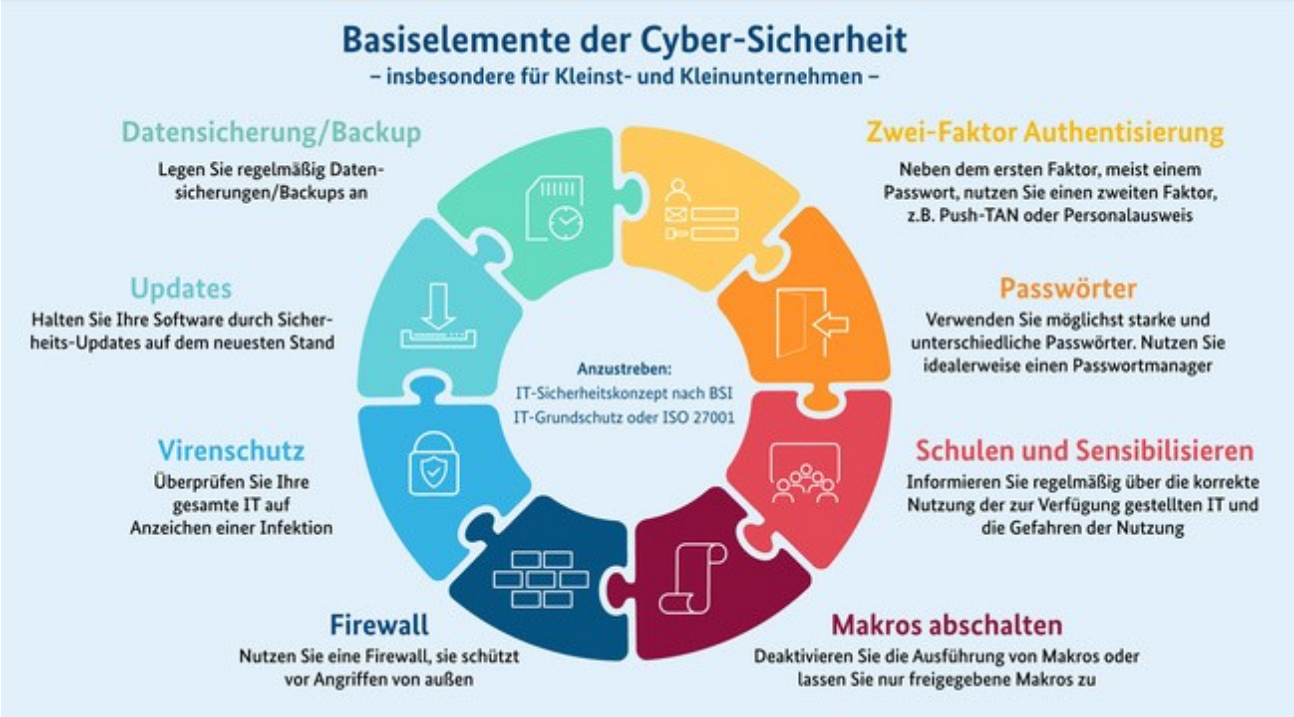

Schaubild: Quelle: Bundesamt für Sicherheit in der Informationstechnik

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

2 *BSI: „Leichter Einstieg“*

CC BY SA

(b) BSI IT-Grundschutz (mit Branchenprofilen)

Das BSI hat über 25 Jahre einen oder den IT-Grundschutz[3] entwickelt und entwickelt diesen nach dem Stand der Technik weiter. Der IT-Grundschutz ist praxisnahe im modularen Bausteinsystem zu allen relevanten Themen aufgebaut und bietet konkrete Sicherheitsanforderungen nach entsprechenden Branchenprofilen. Aus einer Schulung zum Basiswissen BS / IT-Grundschutz habe ich hier eine kurze und knappe Zusammenfassung (Management-Information) zusammengestellt: https://volkerschroer.de/DSGVO/BSI.Basiswissen.IT-Grundschutz.pdf.

v. Falscher Empfänger personenbezogener Daten

„Keiner ist perfekt“ (!), insbesondere in der digitalen Kommunikation, z. B. ist bei Mails schnell der falsche Adressat eingetragen und die Daten sind raus. Eine klassische Datenschutzverletzung. Wie damit umgehen?

(a) Für den Versender

Nach Art.33 DS-GVO sind Datenschutzverletzung innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde zu melden, es sei denn, dies führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen. Besteht ein hohes Risiko, hat nach Art.34 DS-GVO der Verantwortliche die betroffene Person unverzüglich von der Verletzung zu informieren. Ein mögliches Vorgehen:

- ✔ Schaden begrenzen: Mit dem Empfänger umgehend in Kontakt treten und ihn bitten, die Mail / Daten sofort ungesehen / ungenutzt zu vernichten und dies zu bestätigen, sofern nicht selbstständig die Daten gelöscht, verschlüsselt oder anderweitig vernichtet oder vor Zugriffen geschützt werden können.
- ✔ Risiken einschätzen: Welche Risiken können aus dem Verlust der Daten entstehen, wie mögliche finanzielle Schäden, Identitätsdiebstahl, Ruf-/Imageschäden, Bloßstellung, Geheimnisoffenbarung, Existenzgefährdung oder sind es eher geringe bis keine Auswirkungen. Am besten die Einschätzung mit einem Datenschutzbeauftragten vornehmen, bzw. abstimmen. Für Interessierte hat die Datenschutzkonferenz des Bundes und der Länder ein „Kurzpapier“ herausgegeben.[4]
- ✔ Betroffene informieren: Nach meiner Einschätzung ist es immer eine gute Maßnahme, die Betroffenen zu informieren, und zwar unabhängig von der Pflicht bzw. der Risikogewichtung. Neben Offenheit / Transparenz besteht gleichzeitig die Möglichkeit, nach der Risikoeinschätzung der Betroffenen aus einem möglichen Datenverlust zu fragen.
- ✔ Wiederholung vermeiden: Können Maßnahmen ergriffen werden, um solche Vorfälle künftig zu vermeiden (!)?
- ✔ Dokumentation & Meldung: Sind 🟢 geringe bis keine Schäden zu erwarten (z. B. fehlgeleitete Einladungsmail) sollte der Vorgang in einer kurzen Notiz mit den getroffenen Maßnahmen festgehalten werden. Ab einem zu erwartenden 🟡 mittleren Risiko besteht Meldepflicht gegenüber der zuständigen Aufsichtsbehörde und bei zu erwartendem 🟠 hohen Risiko die Pflicht zur Information der Betroffenen. Eine kurze Zusammenfassung (1. Seite) zur „Meldung einer Schutzverletzung“[5] und eine Checkliste zum Ausfüllen und Erstellung einer Meldung an die Aufsichtsbehörde einschließlich zur eigenen Dokumentation[6] finden Sie auf meiner Website.

3 BSI: *„IT-Grundschutz, Informationssicherheit mit System“*

4 Quelle: DSK: „Kurzpapier Nr. 18 *„Risiko für die Rechte und Freiheiten natürlicher Personen““*

5 LINK: *Datenschutzverletzung – Information (12/2022) - PDF*

6 LINK: *Vorlage Checkliste und Meldung (12/2022) - PDF*

CC BY SA

(b) Für den Empfänger[7]

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

Werden die Daten allerdings (natürlich) versehentlich selbst in eigenen Systemen verarbeitet, fällt dies möglicherweise unter die Aufbewahrungspflichten der Abgabenordnung §147 AO oder §257 HGB. Der Rechtsgrund der Verarbeitung ergibt sich dann aus Art.6 Abs.1c DS-GVO mit einer Löschfrist nach Art.17 Abs.3b. Nach den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) lautet es unter 11.2 (Nr. 172):[8]

> *Enthalten elektronisch gespeicherte Datenbestände z. B. nicht aufzeichnungs- und aufbewahrungspflichtige, personenbezogene oder dem Berufsgeheimnis (§102 AO) unterliegende Daten, so obliegt es dem Steuerpflichtigen oder dem von ihm beauftragten Dritten, die Datenbestände so zu organisieren, dass der Prüfer nur auf die aufzeichnungs- und aufbewahrungspflichtigen Daten des Steuerpflichtigen zugreifen kann. Dies kann z. B. durch geeignete Zugriffsbeschränkungen oder „digitales Schwärzen“ der zu schützenden Informationen erfolgen. Für versehentlich überlassene Daten besteht kein Verwertungsverbot.*

Handelt es sich mit der eigenen Verarbeitung also um nicht aufzeichnungs- bzw. aufbewahrungspflichtige Daten / Unterlagen, können diese gelöscht bzw. vernichtet werden. Zur Sicherheit kann eine neutrale Notiz dazu nicht schaden. In allen anderen Fällen sollten die Daten zu Personen bzw. Berufsgeheimnissen gezielt gelöscht und unkenntlich gemacht werden, auf jeden Fall sind diese für die weitere Verarbeitung zu sperren, Zugriffsrechte zu minimieren und nach Ablauf der gesetzlichen Aufbewahrungsfrist direkt zu löschen.

vi. Die Sache mit dem „berechtigten Interesse“[9]

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

> *„die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.“*

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

(a) Was ist „berechtigtes Interesse“?

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

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

Dank des Gesetzes gegen den unlauteren Wettbewerb und des Tele-Medien-Gesetzes muss die Möglichkeit bestehen, diese Sammlung zu unterbinden (PS: Allerdings war es jetzt am Fernseher mühsam, jeden einzelnen abzuwählen). ErwG (48) enthält ein „kleines Konzernprivileg“ dazu,

7 Quelle: Dr.Datenschutz: „Fehlversand: Wie umgehen mit aufgezwungenen Daten“

8 Quelle: BMF Amtliches AO-Handbuch

9 Quelle: Deutsche Gesellschaft für Datenschutz: „Wie kann diese Rechtsgrundlage zur Rechtfertigung für Verarbeitung...“

CC BY SA

bezüglich der Verarbeitung innerhalb einer zentrierten Unternehmensgruppe, allerdings nicht über Grenzen hinweg. ErwG (39) besagt, dass personenbezogene Daten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch mildere Mittel erreicht wird.

(b) Aber: Die Abwägung ist zwingend

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

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

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

vii. „Haushaltsausnahme“, was ist PRIVAT?

(a) Fazit:

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

(b) Regelung DSGVO

Sachlicher Anwendungsbereich Art.2 Abs.2c DSGVO:

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

Erwägungsgrund (18) DSGVO:

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

(c) ● Die DSGVO findet keine Anwendung ...

- ✔ … auf private Adress- und Telefonverzeichnisse (z. B. im Smartphone), sofern kein Bezug zu beruflicher oder wirtschaftlicher Tätigkeit besteht.
- ✔ … auf Social-Media-Accounts, wenn diese ausschließlich dem Zweck der Darstellung der eigenen Person dienen und ausschließlich im Rahmen persönlicher oder familiärer Tätigkeit erfolgt.
- ✔ … auf Urlaubsfotos, Videos und anderen Aufnahmen von Familie und Freunden, wenn diese ausschließlich diesem Personenkreis zur Verfügung stehen, worauf zu achten ist (! keine Bekannten von Bekannten des Personenkreises, wie in Einstellungen in Social-Media-Accounts).
- ✔ Wenn es eine im Umfang „geübte, regelmäßige Praxis“ ist, den Betroffenen lange bekannt, ersichtlich und kein Widerspruch erfolgte, dürfte eine spätere Beschwerde / Schadenersatzforderung schwer geltend machen zu sein. Gleiches gilt für eine Einwilligung im

CC BY SA

Gespräch, oder die Preisgabe der Kontaktdaten zur Verarbeitung im Adressbuch des Smartphones, oder die Übergabe einer Visitenkarte u. ä.

(d) Die DSGVO findet Anwendung ...

✗ … bei Veröffentlichung an einen größeren Empfängerkreis außerhalb des persönlichen Umfeldes, z. B. Follower, Freunde und deren Follower und Freunde auf Social-Media-Accounts, oder eine Veröffentlichung auf Videoplattformen mit der Möglichkeit zu teilen. Bei virtuellem Freundeskreis und nicht exklusiven Followern wird es schwierig eine Abgrenzung zum persönlichen, familiären Kreis zu treffen bzw. diesen einzuhalten (Urteil EuGH C-345/17 Feb. 2019)[10]. Zur Vermeidung von Problemen sollte vorab eine Einwilligung der Beteiligten zur Veröffentlichung eingeholt werden (mündlich ausreichend, schriftlich besser nachweisbar).

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

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

✗ … bei Kamerasystemen, die den öffentlichen Bereich erfassen. Dazu der EuGH[11]:

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

➢ Rechtlich nicht abschließend geklärt sind Aufnahmen von Dashcams. Aus dem Beitrag des ADAC[12] zu diesem Thema ist zusammenfassend festzuhalten. Grundsätzlich sind permanente, anlasslose Aufzeichnung auch als „Hilfssheriff für Verkehrsverstöße“ verboten. Aber, kurze anlassbezogene Aufnahmen (keine Daueraufnahme und/oder Dauerspeicherung LOOP-Funktion) von Unfällen können als Beweis verwertbar sein.

viii. 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.1[13] 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 DS-GVO und das TTDSG zu beachten. Da E-Mail-Marketing also per se nicht erlaubt ist, wird eine Einwilligung[14] / Zustimmung inklusive aller Informationspflichten[15] des Empfängers benötigt und zwar bevor die erste E-Mail versandt wird.

(a) 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.

10 *Quelle: InfoCuria: „EuGH C-345/17 vom 14.02.2019“*
11 *Quelle: InfoCuria: „EuGH C-212/13 vom 11.12.2014“*
12 *Quelle: ADAC: „Dashcams. Was erlaubt ist und was nicht“*
13 *Quelle: https://dejure.org/gesetze/UWG/7.html*
14 *Quelle: Einwilligung: DS-GVO Art.4 Nr.11 https://dejure.org/gesetze/DSGVO/4.html*
15 *Quelle: Informationspflichten: DS-GVO Art.13, 14, 15 https://dejure.org/gesetze/DSGVO/13.html*

CC BY SA

- 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.

(b) 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.

ix. 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-NRW[16] 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 Betroffenenrisiko: Mindestenderfordernis ist der Aufbau einer gesicherten TLS – Verbindung (STARTTLS; SMTPS).
- ✔ Hohes Betroffenenrisiko: 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 Aufsichtsbehörden[17] 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.

16 *LfDI-NRW: „Technische Anforderungen an technische und organisatorische Maßnahmen beim E-Mail-Versand“*

17 *DSK: „Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen ... auf ausdrücklichen Wunsch“*

CC BY SA

Für einen Verzicht („nur“ TLS – Verschlüsselung) sollte in aufklärender Weise über die Risiken eine Einwilligung eingeholt werden. Bei sehr hohem Betroffenenrisiko ist nicht auf eine End-to-End Verschlüsselung zu verzichten!

x. 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-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“[18] veröffentlicht. Daraus kurz zusammengefasst:

(a) 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.

(b) Alternative: Dezentrale PeerTube-Instanz[19]

Laut LfDI-BW eine nicht kommerzielle, datenschutzkonforme Alternative mit Interaktionen, da kein zentraler Anbieter, sondern viele einzelne PeerTube - Server. Nach tagesschau – Faktenfinder[20], **allerdings** eine Alternative mit Tücken, da u. a. IP-Adressen öffentlich werden und jeder für die Einhaltung der Gesetze selbst verantwortlich ist.

(c) 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.

(d) 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 Datenschutzanforderungen gleich denen Fotoaufnahmen für Personen[21] und Mitarbeiter[22] strikt zu beachten.

Bei Bedarf, einfach einmal sprechen!

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.

18 *Quelle: LfDI – Baden-Württemberg: „Einbindung von Videos in eigene Webseiten“*
19 *Link: PeerTube-Instanz: https://joinpeertube.org/instances*
20 *Quelle: tagesschau>faktfinder>peertube*
21 *Quelle. Jahresübersicht Datenschutzinfo 2021: „Was ist jetzt mit Fotos“, Seite 16*
22 *Quelle: Jahresübersicht Datenschutzinfo 2022: "Mitarbeiter Information & Einwilligung(en)", Seite 6*