Datenschutz und IT-Compliance

Das Handbuch für Admins und IT-Leiter

DIE LESEPROBE

Kapitel 5
Datenschutzverpflichtungen als Unternehmen umsetzen

Unternehmen unterliegen zahlreichen Verpflichtungen bei der Verarbeitung personenbezogener Daten. In diesem Kapitel lernen Sie die wichtigsten kennen und erhalten Hinweise zur konkreten Umsetzung in der Praxis.

Der Aufbau eines effektiven Datenschutzmanagement-Systems zur Umsetzung von Datenschutzverpflichtungen im Unternehmen beginnt in der Regel mit der Erstellung bzw. Pflege eines Verarbeitungsverzeichnisses, in dem möglichst alle Verarbeitungen von personenbezogenen Daten im Unternehmen dokumentiert sind (siehe Abschnitt 5.1). Daneben müssen Sie auch technische und organisatorische Maßnahmen (TOM)[1] zum Schutz der Daten festlegen und dokumentieren (siehe Abschnitt 5.2).

Von zentraler Bedeutung ist die Erfüllung der Informationspflichten gegenüber Betroffenen (siehe Abschnitt 5.3), die über diverse Rechte, die sogenannten Betroffenenrechte, verfügen, von denen das Auskunftsrecht in der Praxis von besonderer Bedeutung ist (siehe Abschnitt 5.4).

Verarbeiten Sie die Daten nicht selbst, weil Sie einen Dienstleister einsetzen, handelt es sich meist um sogenannte Auftragsverarbeitungen, bei denen externe Dienstleister die Daten auf der Grundlage eines Auftragsverarbeitungsvertrags im Auftrag des Unternehmens verarbeiten (siehe Abschnitt 5.5).

Bei besonders riskanten Verarbeitungen ist die Durchführung einer Datenschutz-Folgenabschätzung erforderlich (Abschnitt 5.6).

Schließlich muss sich jedes Unternehmen – unabhängig von den meisten sonstigen Datenschutzverpflichtungen – die Frage stellen, ob es einen Datenschutzbeauftragten benennen muss (siehe Abschnitt 5.7).

1 Siehe Kapitel 3, »Technischer Datenschutz: Anforderungen der DSGVO an den IT-Betrieb«.

5.1 Bestandsaufnahme der Daten im Unternehmen: So erstellen Sie ein Verarbeitungsverzeichnis (VVT)

Das *Verzeichnis von Verarbeitungstätigkeiten*, häufig kurz *Verarbeitungsverzeichnis* oder noch kürzer *VVT* genannt, ist das Herzstück jedes Datenschutzmanagement-Systems, weil es einen Überblick über sämtliche Verarbeitungstätigkeiten in einem Unternehmen gibt. Es ist auch eine von vielen Dokumentationspflichten, die sich aus der DSGVO für Ihr Unternehmen ergeben, damit Sie Ihrer Rechenschaftspflicht nachkommen können. Es dient sowohl dem Verantwortlichen als auch den Aufsichtsbehörden als Ausgangspunkt für eine erste überblicksmäßige Rechtmäßigkeitsprüfung.

5.1.1 Wer muss ein VVT führen?

Die Verpflichtung, ein solches Verzeichnis zu führen, ergibt sich aus Art. 30 DSGVO und besteht unabhängig davon, ob in Ihrem Unternehmen ein *Datenschutzbeauftragter* (*DSB*) benannt ist oder nicht. Insoweit besteht sehr häufig die Fehlvorstellung in kleineren Unternehmen, dass ein Verarbeitungsverzeichnis nicht geführt werden muss, weil auch keine Verpflichtung zur Benennung eines DSB besteht. Art. 30 DSGVO verpflichtet aber alle Unternehmen, unabhängig von der Größe, der Art und dem Umfang der Verarbeitung personenbezogener Daten, zur Führung eines Verarbeitungsverzeichnisses.

Praxistipp: Ausnahme für Unternehmen mit weniger als 250 Mitarbeitern?

Eine Ausnahme von der Verpflichtung zur Führung eines Verarbeitungsverzeichnisses nach Art. 30 DSGVO enthält Abs. 5. Demnach gelten die in den Absätzen 1 und 2 genannten Pflichten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn, die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich, oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne von Art. 10 DSGVO.

Bei der Mitarbeiterzahl kommt es auf die Kopfzahl der beschäftigten Personen an; es spielt keine Rolle, ob diese auch alle mit der Verarbeitung personenbezogener Daten zu tun haben.

Die Ausnahme greift in der Praxis fast nie. Zum einen ist kaum eine Verarbeitung personenbezogener Daten denkbar, die keinerlei Risiko für die Rechte und Freiheiten der betroffenen Person birgt. Nach dem Wortlaut ist nämlich gerade kein gesteigertes oder hohes Risiko erforderlich, um die Ausnahme entfallen zu lassen; es reicht jegliches Risiko. Die gesamte DSGVO ist von dem Gedanken geprägt, dass eine Verar-

beitung personenbezogener Daten in der Regel mit einem Risiko für die betroffenen Personen einhergeht. Verarbeitungen ohne jegliches Risiko wird es praktisch kaum geben, weshalb teilweise angenommen wird, dass der Wortlaut dahingehend einschränkend auszulegen ist, dass eine Verarbeitung mit lediglich geringem Risiko die Ausnahme erfüllt.

Zum anderen gibt es praktisch kein Unternehmen, das personenbezogene Daten nur gelegentlich verarbeitet. Insbesondere Kunden- und Beschäftigtendaten werden in nahezu jedem Unternehmen regelmäßig verarbeitet.

Im Rahmen der Verarbeitung von Beschäftigtendaten werden zudem in aller Regel auch besondere Kategorien von personenbezogenen Daten gemäß Art. 9 DSGVO verarbeitet (z. B. das Merkmal der Religionszugehörigkeit zum Zwecke der Abführung von Kirchensteuer), weshalb jedes Unternehmen mit Beschäftigen schon aus diesem Grund von der Ausnahme nicht erfasst wird.

5.1.2 Wer hat Einblick in das VVT?

Das VVT müssen Sie nach den Regelungen der DSGVO übrigens nur einem relativ kleinen Personenkreis zugänglich machen. Zugriff hat derjenige, der das VVT erstellt bzw. führt, der DSB, die Geschäftsleitung und auf Anfrage auch die Aufsichtsbehörden (Art. 30 Abs. 4 DSGVO). Das Zurverfügungstellen des Verarbeitungsverzeichnisses kann je nach Ausgestaltung der Anfrage z. B. durch Einsichtnahme vor Ort, postalische oder elektronische Übersendung sowie durch die Erteilung einer Zugangsberechtigung zu einem Datenraum oder zur verwendeten Software erfolgen.

Sollten Sie vielleicht noch das sogenannte *Jedermannsverzeichnis* kennen: Dieses im BDSG a. F. noch vorgesehene Verzeichnis war eine sehr abgespeckte Version des damals *Verfahrensverzeichnis* genannten Vorläufers des VVT, das jedermann auf Anforderung zur Verfügung zu stellen war; es ist ersatzlos entfallen.

5.1.3 Wie wird ein VVT erstellt und gepflegt?

Bevor wir uns den inhaltlichen Anforderungen an ein VVT zuwenden, möchten wir Sie darauf hinweisen, dass es häufig in der Praxis gar nicht so leicht ist, ein vollständiges und aktuelles VVT zu führen. Bereits bei der erstmaligen Erstellung treffen Sie möglicherweise auf Schwierigkeiten, alle Verarbeitungen in einem Unternehmen zu identifizieren. Häufig fehlt die notwendige Unterstützung aus den verschiedenen Abteilungen, weil die Arbeit an einem VVT nicht selten als verschwendete Zeit angesehen wird.

Und selbst wenn Sie alle Hürden genommen und ein VVT erstellt haben, gerät es danach allzu oft in Vergessenheit und wird nicht gepflegt. Sie sollten daher Prozesse

festlegen, die dazu führen, dass der für das VVT Verantwortliche von Änderungen an bestehenden Verarbeitungen Kenntnis erlangt und neu eingeführte Verarbeitungen auch in das VVT aufgenommen werden. Empfehlenswert ist die Festlegung von festen Zeitabständen für die Überprüfung der Aktualität des VVT. Mindestens einmal im Jahr sollten Sie das VVT durchgehen[2] und prüfen, ob sich Änderungen an bestehenden Verarbeitungen ergeben haben oder neue Verarbeitungen eingeführt wurden.

Eine Versionierung ist nicht vorgeschrieben, aber sehr hilfreich, und auch ältere Versionen sollten im Archiv vorgehalten werden, falls sich die Anfrage einer Aufsichtsbehörde einmal auf eine frühere Verarbeitung, die zwischenzeitlich aus dem VVT entfernt oder die geändert wurde, beziehen sollte.

Tipp: Bleiben Sie unbedingt hartnäckig!

Wenn Sie ein VVT erstellen sollen/müssen, bleiben Sie hartnäckig, bis Sie alle erforderlichen Informationen haben. Und wenn Sie das VVT nicht selbst erstellen sollen/müssen, beantworten Sie die an Sie gerichteten Fragen vollständig und zeitnah.

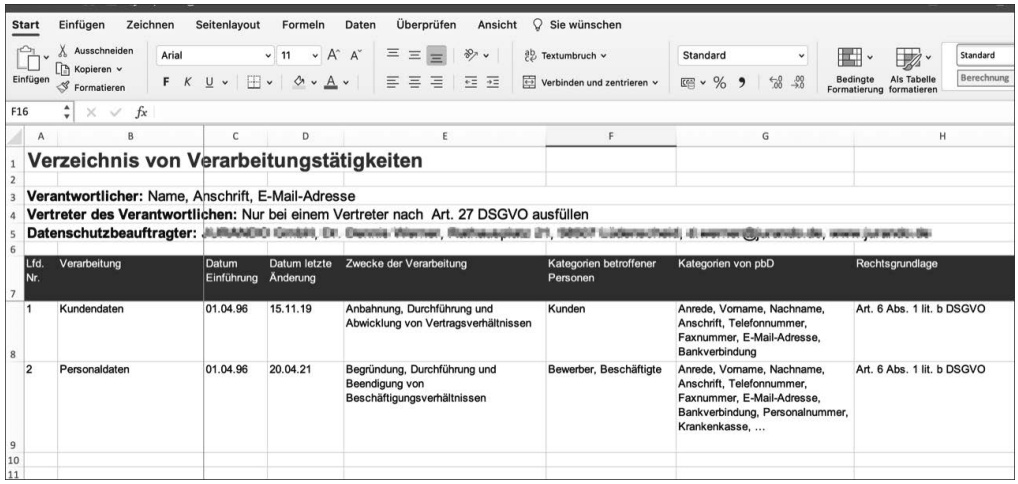
Die Pflicht, ein VVT zu führen, trifft nach dem Wortlaut der DSGVO in Art. 30 den Verantwortlichen bzw. den Auftragsverarbeiter. In der Praxis wird das VVT häufig vom DSB erstellt und gepflegt. Allerdings gehört es gerade nicht zu den gesetzlichen Pflichten des DSB, das VVT zu erstellen und zu führen. Man sollte also mit dem DSB eine klare Vereinbarung darüber treffen, wer das VVT erstellt und pflegt. Zu dieser Frage sollte es daher z. B. eine klare Reglung im Vertrag mit dem DSB geben.

Zweigniederlassungen und unselbständige Zweigstellen gehören datenschutzrechtlich zum Verantwortlichen und müssen deshalb kein eigenes VVT führen. Ihre Verarbeitungen sind im VVT des Verantwortlichen zu dokumentieren. Anders sieht es bei rechtlich selbständigen Gesellschaften eines *Konzerns* bzw. einer *Unternehmensgruppe* aus. Hier ist jedes Konzernunternehmen eigenständig verantwortlich und muss auch ein eigenes VVT führen. Natürlich kann die Muttergesellschaft bei gleichgelagerten Verarbeitungstätigkeiten Muster zur Verfügung stellen und so eine einheitliche Struktur der Verarbeitungsverzeichnisse im Konzern sicherstellen.

Art. 30 Abs. 3 DSGVO verpflichtet Sie, das VVT schriftlich zu führen. Das bedeutet aber nicht, dass Sie es auf Papier führen müssen. Die DSGVO gibt Ihnen ausdrücklich auch die Möglichkeit, es in einem elektronischen Format zu führen. Die elektronische Führung dürfte die absolute Regel sein, was natürlich nicht ausschließt, dass das VVT z. B. für ein Datenschutzhandbuch auch ausgedruckt werden kann. Führend sollte aber immer die elektronische Form sein.

2 Vergleiche dazu auch den Prozess zur Risikobewertung in Kapitel 3, »Technischer Datenschutz: Anforderungen der DSGVO an den IT-Betrieb«.

Bei der Wahl des Formats sind Sie völlig frei. Gebräuchlich sind Word- bzw. Excel-Dokumente (siehe Abbildung 5.1), aber auch spezielle Datenschutzmanagement-Software.



Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher: Name, Anschrift, E-Mail-Adresse
Vertreter des Verantwortlichen: Nur bei einem Vertreter nach Art. 27 DSGVO ausfüllen
Datenschutzbeauftragter: [redacted]

Lfd. Nr.	Verarbeitung	Datum Einführung	Datum letzte Änderung	Zwecke der Verarbeitung	Kategorien betroffener Personen	Kategorien von pbD	Rechtsgrundlage
1	Kundendaten	01.04.96	15.11.19	Anbahnung, Durchführung und Abwicklung von Vertragsverhältnissen	Kunden	Anrede, Vorname, Nachname, Anschrift, Telefonnummer, Faxnummer, E-Mail-Adresse, Bankverbindung	Art. 6 Abs. 1 lit. b DSGVO
2	Personaldaten	01.04.96	20.04.21	Begründung, Durchführung und Beendigung von Beschäftigungsverhältnissen	Bewerber, Beschäftigte	Anrede, Vorname, Nachname, Anschrift, Telefonnummer, Faxnummer, E-Mail-Adresse, Bankverbindung, Personalnummer, Krankenkasse, ...	Art. 6 Abs. 1 lit. b DSGVO

Abbildung 5.1 Beispiel für ein VVT in Excel

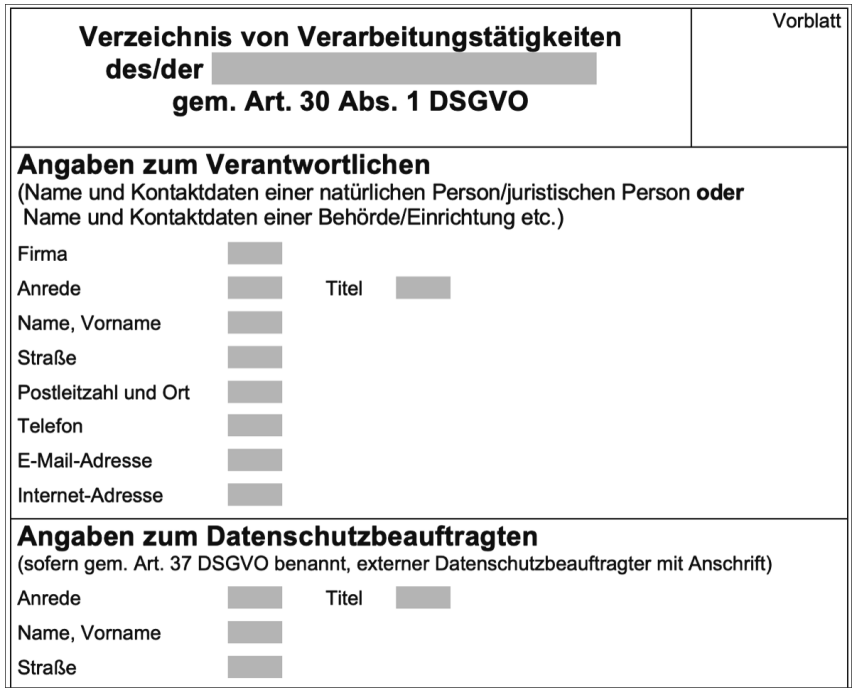
Die Aufsichtsbehörden stellen Ihnen auch Muster bereit.[3] Diese gehen allerdings teilweise über den gesetzlichen Mindestinhalt hinaus. Dies ist an bestimmten Stellen sinnvoll und an anderen Stellen weniger sinnvoll. In größeren Unternehmen kann es z. B. sehr hilfreich sein, auch die jeweils verantwortliche Fachabteilung mit einem Ansprechpartner und Kontaktdaten aufzunehmen. Die Muster können aber in jedem Fall gut als Orientierungshilfe bei der Erstellung des eigenen VVT herangezogen werden. Zweckmäßig ist es eigentlich immer, bestimmte Angaben, die für alle Verarbeitungen gleich sind, wie z. B. den Namen und die Kontaktdaten des Verantwortlichen, auf einem »Vorblatt« voranzustellen (siehe Abbildung 5.2). Neben den Mustern der Aufsichtsbehörden gibt es auch das Kurzpapier Nr. 1 der Datenschutzkonferenz (DSK), das sich mit dem VVT beschäftigt.[4]

In welcher *Sprache* das Verzeichnis geführt werden muss, ist in der DSGVO nicht geregelt. Aus Praktikabilitätsgründen empfiehlt es sich, dass Verzeichnis in der Sprache der zuständigen Aufsichtsbehörde zu verfassen. Alternativ kann in internationalen Konzernen auch z. B. die englische Sprache verwendet werden, wobei sich der Verantwortliche, der seinen Sitz in Deutschland hat, darüber bewusst sein muss, dass

3 Ein Beispiel für ein solches Muster finden Sie auf den Seiten des Landesbeauftragten für Datenschutz und Informationsfreiheit NRW (LDI) unter *www.ldi.nrw.de/datenschutz/verwaltung/verarbeitungsverzeichnis* (zuletzt aufgerufen am 15. Juni 2023).

4 Die Kurzpapier der DSK finden Sie unter *www.datenschutzkonferenz-online.de/kurzpapiere.html* (zuletzt aufgerufen am 15. Juni 2023).

die Aufsichtsbehörde gegebenenfalls eine Übersetzung verlangen kann (§ 23 Abs. 2 S. 1 Verwaltungsverfahrensgesetz, VwVfG).



Verzeichnis von Verarbeitungstätigkeiten
des/der
gem. Art. 30 Abs. 1 DSGVO

Vorblatt

Angaben zum Verantwortlichen
(Name und Kontaktdaten einer natürlichen Person/juristischen Person **oder** Name und Kontaktdaten einer Behörde/Einrichtung etc.)

Firma
Anrede
Titel
Name, Vorname
Straße
Postleitzahl und Ort
Telefon
E-Mail-Adresse
Internet-Adresse

Angaben zum Datenschutzbeauftragten
(sofern gem. Art. 37 DSGVO benannt, externer Datenschutzbeauftragter mit Anschrift)

Anrede
Titel
Name, Vorname
Straße

Abbildung 5.2 Beispiel für ein Vorblatt bei einem in Word geführten VVT, orientiert am Muster des LDI

5.1.4 Gesetzliche Mindestinhalte des VVT

Die Inhalte des VVT eines Verantwortlichen unterscheiden sich leicht von den Inhalten des VVT eines Auftragsverarbeiters. Der jeweilige Mindestinhalt ist für den Verantwortlichen in Art. 30 Abs. 1 DSGVO und für den Auftragsverarbeiter in Art. 30 Abs. 2 DSGVO vorgegeben.

Mindestinhalte des VVT eines Verantwortlichen

Inhaltlich muss das VVT eines Verantwortlichen mindestens die in Art. 30 Abs. 1 DSGVO aufgezählten Punkte enthalten.

Praxistipp: Mindestinhalt eines VVT nach Art. 30 Abs. 1 DSGVO für Verantwortliche

- Name und Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten

- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfängern in Drittländern oder internationale Organisationen
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Unterabs. 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO

Wir gehen diese Punkte nun im Einzelnen durch. Den ersten Punkt, also den Namen und die Kontaktdaten des Verantwortlichen, eines gemeinsam Verantwortlichen und des DSB ziehen Sie am besten vor die Klammer auf ein gesondertes Vorblatt oder in den Kopf einer Excel-Tabelle, weil diese Angaben für alle Verarbeitungen gleich sind.

Der *Name des Verantwortlichen* ist in der Regel die Firma des Unternehmens mit Rechtsformzusatz. Die Firma ist der Name des Unternehmens, also z. B. »Muster Maschinen«. Der Rechtsformzusatz beschreibt – wie der Name schon sagt – die Rechtsform des Unternehmens und damit vor allem die Haftungsverhältnisse, also z. B. GmbH. Zusammen lautet der Name dann korrekt: »Muster Maschinen GmbH«. Weitere verbreitete Rechtsformen sind e. K., OHG, KG und GmbH & Co. KG. Unzureichend wäre deshalb z. B. »Muster & Co.«, weil es sich dann sowohl um eine OHG als auch um eine KG handeln könnte. Wenn man es ganz besonders präzise machen möchte, kann man die Handelsregisternummer und das Amtsregister, bei dem die Firma registriert ist, aufnehmen (z. B. »Amtsgericht Musterstadt, HRB 12345«).

Die *Kontaktdaten* müssen angegeben werden, um eine effektive Erreichbarkeit zu gewährleisten. Mindestens sollten Sie deshalb die postalische Anschrift und eine E-Mail-Adresse angegeben. Sinnvoll kann auch eine Telefonnummer sein.

Nicht zwingend müssen Sie den Namen des Inhabers oder Geschäftsführers angeben. Schädlich ist eine entsprechende Angabe aber nicht. Allerdings wechselt die Person des Geschäftsführers meistens häufiger als die postalische Anschrift oder die E-Mail-Adresse. Da das VVT laufend aktuell gehalten werden muss, sollten Sie immer überlegen, ob eine bestimmte Eintragung wirklich zwingend notwendig ist, weil man

im Falle einer Aufnahme in das VVT die Aktualität der Angabe laufend überwachen muss. Für den *gemeinsam Verantwortlichen* gilt das Gleiche. Wer ein gemeinsamer Verantwortlicher ist, erfahren Sie an anderer Stelle.[5]

Der *Vertreter des Verantwortlichen* ist übrigens nicht das Vertretungsorgan des Unternehmens, also z. B. nicht der Geschäftsführer einer GmbH. Gemeint ist der Vertreter eines nicht in der EU niedergelassenen Verantwortlichen. Ein solcher hat nach Art. 27 DSGVO einen inländischen Vertreter zu benennen. Mit einer solchen Konstellation werden Sie selten zu tun haben. Und wenn doch, sollten Sie im Zweifel einen Datenschutzexperten zurate ziehen.

Zuletzt bleibt der *Datenschutzbeauftragte*. Auch diesen müssen Sie namentlich und mit Kontaktdaten aufführen. Hier besteht ein interessanter Unterschied zu den Informationspflichten nach Art. 13 DSGVO, also den Datenschutzinformationen, die Sie den Betroffenen zur Verfügung stellen müssen: Im Rahmen der Datenschutzinformationen müssen Sie nur die Kontaktdaten des DSB, nicht aber dessen Name, mitteilen.[6]

Praxistipp: Beispiel für Angaben auf einem Vorblatt

Verantwortlicher:

Muster Maschinen GmbH, Musterstraße 1, 12345 Musterstadt, *info@example.com*

Datenschutzbeauftragter:

Max Mustermann, Musterstraße 1, 12345 Musterstadt, *m.mustermann@example.com*

Nachdem Sie damit das Vorblatt mit den allgemeinen Informationen vollständig erstellt haben, geht es nun zu den einzelnen *Verarbeitungen*. Es ist sinnvoll, für jede einzelne Verarbeitung ein gesondertes Blatt anzulegen bzw. eine eigene Zeile in einer Excel-Tabelle vorzusehen. An dieser Stelle stellt sich dann die Frage, was eine Verarbeitung ist. Ein Beispiel: Eine Verarbeitung könnte die Personaldatenverarbeitung sein. Eine Verarbeitung könnte aber auch z. B. das Bewerbermanagement, die Lohnbuchhaltung oder die Ehrung von langjährig Betriebszugehörigen sein. Die DSGVO schreibt keine bestimmte Detailtiefe des VVT vor. Wer es »quick and dirty« mag, der fasst mehrere Verarbeitungen aus einem Bereich unter einem Oberbegriff zusammen und gelangt so relativ schnell zu einem umfassenden VVT. Allerdings sind die Angaben in einem solchen VVT meist sehr grob und wenig aussagekräftig. Für den Anfang kann das aber ein probates Mittel sein, um überhaupt erst einmal zu einem vollständigen VVT zu kommen. Da ein VVT sowieso laufend weitergeführt werden muss, kann der Detailgrad dann nach und nach erhöht werden.

5 Siehe dazu Kapitel 1, »Grundlagen: Was Sie über den Datenschutz wissen müssen«.
6 Siehe dazu auch Kapitel 5, »Datenschutzverpflichtungen als Unternehmen umsetzen«.

Praxistipp: Beispiel für ein grobes VVT

- Personaldatenverarbeitung
- Kundendatenverarbeitung
- Marketing

Praxistipp: Beispiel für ein ausdifferenziertes VVT

- Personaldatenverwaltung
  - Bewerbermanagement
  - Personalaktenführung
  - Lohnbuchhaltung
  - Zeiterfassung
  - Flottenmanagement
  - Ehrung langjährig Betriebszugehöriger
  - ...
- Kundendatenverarbeitung
  - CRM-System
  - Buchhaltung
  - Vertragsabwicklung
  - ...
- Marketing
  - Website
  - Social-Media-Kanäle
  - Newsletter
  - Direktwerbung
  - ...

Ein wichtiger Grundsatz der DSGVO ist die *Zweckbindung*. Deshalb muss bei jeder Verarbeitung der *Zweck* dokumentiert werden. Die Beschreibung des Zwecks sollte möglichst präzise und aussagekräftig sein. Völlig allgemeingehaltene Zwecke, wie z. B. die Steigerung des Unternehmensgewinns, sind unzureichend.

Praxistipp: Beispiele für die Zwecke einer Verarbeitung

- Entscheidung über Einstellung bzw. Ablehnung im Bewerbungsverfahren
- Auszahlung von Löhnen und Gehältern
- Ausführen von Bestellungen des Kunden
- Bearbeitung von Gewährleistungsansprüchen
- Werbung für eigene und ähnliche Produkte gegenüber Bestandskunden
- Neukundengewinnung

Es folgt die abstrakte Beschreibung der *Kategorien betroffener Personen*. Aus dem Begriff *Kategorie* lässt sich ableiten, dass nicht einzelne Personen namentlich aufgeführt werden sollen, sondern eine Zusammenfassung zu Gruppen mit gemeinsamen Merkmalen erfolgen muss. Eine Verarbeitung kann auch mehrere Personengruppen betreffen. Es sind dann alle betroffenen Personengruppen bei der Verarbeitung aufzuführen.

Praxistipp: Beispiele für Kategorien betroffener Personen

- Bewerber
- Mitarbeiter
- Interessenten
- Kunden
- Lieferanten
- Patienten

Falls Ihr Unternehmen Daten von *Kindern* verarbeitet, empfiehlt es sich, diese immer als gesonderte Personengruppe aufzuführen, da Kinder in der DSGVO als besonders schutzwürdig eingestuft werden und beim Umgang mit Daten von Kindern meist besondere Anforderungen zu beachten sind.

Den Kategorien von betroffenen Personen müssen *Kategorien personenbezogener Daten* zugeordnet werden, damit ersichtlich ist, welche Art von Daten einer Kategorie von Betroffenen verarbeitet wird. Erneut stellt sich die Frage nach der Detailtiefe. Eine Kategorie können Kontaktdaten sein, Kategorien können aber auch Name, Anschrift, E-Mail-Adresse usw. sein.

Die DSGVO selbst kennt im Wesentlichen drei Kategorien von personenbezogenen Daten:

- Zunächst sind das die in Art. 9 Abs. 1 DSGVO aufgezählten *besonderen Kategorien von personenbezogenen Daten*, die die DSGVO als besonders sensibel einstuft. Sie haben diese Daten weiter oben bereits kennengelernt.[7]
- Daneben gibt es als weitere Kategorie *personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten*, die in Art. 10 DSGVO eine eigene Regelung erfahren haben, mit denen Sie aber selten zu tun haben dürften.
- Als letzte Kategorie bleiben dann alle anderen *personenbezogenen Daten*, die weder Art. 9 noch Art. 10 DSGVO unterliegen, wenn Sie so wollen also die große Masse der »normalen« personenbezogenen Daten, die in jedem Unternehmen anfallen und mit denen Sie am meisten umgehen werden.

7 Siehe Kapitel 1, »Grundlagen: Was Sie über den Datenschutz wissen müssen«.

Da die Verarbeitung von personenbezogenen Daten, die Art. 9 oder Art. 10 DSGVO unterliegen, wiederum besonderen Voraussetzungen unterliegt, ist auf diese Art von Daten besonderes Augenmerk zu legen. Es ist deshalb sehr sinnvoll, im VVT deutlich hervorzuheben, wenn eine Verarbeitung derartige Daten betrifft. Die DSGVO fordert diese Differenzierung in Art. 30 DSGVO zwar nicht, sie ist gleichwohl wegen der besonderen Anforderungen, die an eine Verarbeitung dieser Daten gestellt werden, eine sinnvolle Ergänzung des gesetzlichen Mindestinhalts eines VVT.

Praxistipp: Beispiele für Kategorien personenbezogener Daten

- Kontaktdaten
- Geburtsdatum
- Vertragsdaten
- Zahlungsdaten
- IP-Adressen

Als Nächstes sind die Kategorien von *Empfängern* aufzuführen. Empfänger sind nach Art. 4 Nr. 9 DSGVO Stellen, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich um Dritte handelt oder nicht. *Dritte* wiederum sind alle Stellen außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Die Muster mancher Aufsichtsbehörden differenzieren zunächst zwischen internen und externen Empfängern. Interner Empfänger von Bewerbungsunterlagen kann z. B. die Personalabteilung sein. Externer Empfänger von Kundenadressen kann z. B. der Versanddienstleister sein. Zwingend ist die Unterscheidung allerdings nicht. Ob interne Empfänger überhaupt zwingend anzugeben sind, ist umstritten. Schaden kann die Angabe von internen Empfängern aber nicht. Häufig ist die Angabe von internen Empfängern sogar hilfreich, um Datenströme innerhalb eines Unternehmens aufzudecken und bei der Gelegenheit auch direkt zu hinterfragen.

Angegeben werden müssen nur Kategorien und nicht namentlich einzelne Empfänger. Gleichwohl ist es unschädlich, Empfänger namentlich zu benennen. Wenn es nur einen überschaubaren Kreis von Empfängern gibt, kann es sogar ratsam sein, diese namentlich zu benennen. Andererseits führt die namentliche Nennung gegebenenfalls zu einem erhöhten Pflegeaufwand, da die Angabe im VVT angepasst werden muss, wenn z. B. ein Dienstleister ausgewechselt wird.

Ausdrücklich gefordert ist die Angabe von *Empfängern in Drittländern*. Es sollte deshalb bei jedem Empfänger angegeben werden, in welchem Land derjenige seinen Sitz hat. Handelt es sich nämlich um ein Drittland, ist besondere Vorsicht geboten, da an

die Übermittlung von personenbezogenen Daten an ein Unternehmen in einem Drittland in den Art. 44 ff. DSGVO sehr hohe Anforderungen gestellt werden.[8] Es sollte deshalb aus dem VVT auf den ersten Blick ersichtlich sein, wenn ein Empfänger in einem Drittland an der Verarbeitung beteiligt ist.

Praxistipp: Beispiele für Kategorien von Empfängern

- Externe Empfänger
  - Auftragsverarbeiter
  - Marketingagentur
  - Versanddienstleister
  - Steuerberater
  - Finanzbehörden
  - Krankenkassen
- Interne Empfänger
  - Personalabteilung
  - Vertrieb
  - Buchhaltung
  - Betriebsrat

Erfolgt eine *Übermittlung an ein Drittland* oder ist eine solche geplant, muss dies im VVT vermerkt werden. Gemeint ist natürlich nicht die Übermittlung an einen Staat als Empfänger. Sie werden nur sehr selten personenbezogene Daten Ihrer Kunden an die Vereinigen Staaten von Amerika übermitteln. Gemeint ist die Übermittlung in ein Drittland, also z. B. an ein Unternehmen in den USA. Jedes Drittland ist namentlich zu nennen. Schwierig wird es, wenn in dem Empfängerland kein angemessenes Datenschutzniveau gewährleistet ist. Dann sind *geeignete Garantien* in Bezug auf den Schutz der übermittelten personenbezogenen Daten zu ergreifen und im VVT zu dokumentieren. Kommen Sie tatsächlich zu diesem Punkt, sollten Sie einen Datenschutzexperten zurate ziehen, weil derartige Drittlandübermittlungen sehr risikobehaftet sind.

Besonders spannend ist die Verpflichtung, wenn möglich, die vorgesehenen *Fristen für die Löschung der verschiedenen Datenkategorien*, anzugeben. An dieser Stelle ist derjenige fein raus, der ein *Löschkonzept* hat. Dieses haben allerdings – realistisch betrachtet – die wenigsten Unternehmen. Hat Ihr Unternehmen ein Löschkonzept, müssen die darin enthaltenen Angaben im VVT nicht unbedingt wiederholt werden. Im VVT können Sie an dieser Stelle auch einfach auf das Löschkonzept verweisen.

8 Siehe dazu Kapitel 7, »Export von Daten in alle Welt: Was ist erlaubt?«.

Eine explizite Verpflichtung, ein Löschkonzept[9] zu erstellen und zu führen, enthält die DSGVO übrigens nicht. Allerdings lassen sich viele Verpflichtungen aus der DSGVO rund um das Löschen von Daten ohne ein Löschkonzept kaum umsetzen. Das betrifft z. B. den Grundsatz der Speicherbegrenzung aus Art. 5 Abs. 1 lit. e DSGVO und den Anspruch des Betroffenen auf Löschung aus Art. 17 DSGVO genauso wie die hier beschriebene Verpflichtung zur Dokumentation der Löschfristen im VVT.

Ganz allgemein gehaltene Angaben, wie z. B. »Wir löschen Ihre Daten, wenn der Zweck der Verarbeitung erreicht ist und kein gesetzlichen Aufbewahrungsfristen mehr bestehen.«, reichen streng genommen nicht aus. Im Regelfall muss eine konkrete Löschfrist angegeben werden. Diese kann sich natürlich aus gesetzlichen Vorgaben, z. B. in Form von Aufbewahrungsfristen nach der Abgabenordnung (AO) oder dem Handelsgesetzbuch (HGB), ergeben. Personenbezogene Daten, die keiner gesetzlichen Aufbewahrungsfrist unterliegen, sind nach der Zweckerreichung umgehend zu löschen, und zwar unabhängig davon, ob der Betroffene die Löschung verlangt oder nicht.

Zuletzt muss das VVT eine allgemeine Beschreibung der *technischen und organisatorischen Maßnahmen* (*TOM*) nach Art. 32 Abs. 1 DSGVO enthalten.[10] Diese Angaben werden meistens in einem gesonderten Dokument aufgeführt, auf das im VVT verwiesen werden kann. Wenn es über die allgemeinen Maßnahmen hinaus spezielle Vorkehrungen für eine bestimmte Verarbeitung gibt, kann es sich anbieten, diese besonderen Vorkehrungen im VVT bei der entsprechenden Verarbeitung zu dokumentieren. Möglich ist auch der Verweis auf ein *IT-Sicherheitskonzept* oder eine *Zertifizierung nach ISO 27001*.

Sinnvolle Ergänzungen zum gesetzlichen Mindestinhalt

Neben diesem gesetzlichen Mindestinhalt eines VVT gibt es ein paar Punkte, die zusätzlich im VVT dokumentiert werden können und auch sollten, um sich einen vollständigen Überblick über die Rechtmäßigkeit der Verarbeitungen zu verschaffen.

Als Erstes ist hier die *Rechtsgrundlage der Verarbeitung* zu nennen. Sie erinnern sich: Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten, wenn es nicht eine Rechtsgrundlage gibt, die die Verarbeitung ausdrücklich gestattet (sogenanntes Verbot mit Erlaubnisvorbehalt). Sie müssen sich also sowieso bei jeder Verarbeitung genau überlegen, auf welche Rechtsgrundlage die Verarbeitung gestützt werden kann. Das Ergebnis Ihrer Überlegungen sollten Sie dann auch direkt im VVT dokumentieren. Im Rahmen der Informationen, die Sie dem Betroffenen nach Art. 13 DSGVO zur Verfügung stellen müssen, müssen Sie die Rechtsgrundlage zwingend angeben. Noch einmal zur Erinnerung: Rechtsgrundlagen finden Sie vor allem in Art. 6

9 Siehe dazu Kapitel 3, »Technischer Datenschutz: Anforderungen der DSGVO an den IT-Betrieb«.
10 Siehe dazu Kapitel 3.

DSGVO und für Beschäftigtendaten in § 26 BDSG (der nach aktueller Rechtsprechung mindestens teilweise europarechtswidrig sein dürfte). Wird eine Verarbeitung nach Art. 6 Abs. 1 lit. f DSGVO auf ein berechtigtes Interesse des Verantwortlichen gestützt, sollten Sie im VVT auf die dafür erforderliche Interessenabwägung verweisen, die Sie vorgenommen haben.

Sinnvoll kann es daneben sein, bei der Verarbeitung zusätzlich anzugeben, ob ein *Auftragsverarbeiter* eingesetzt wird. Auch vorgenommene *Risikoabschätzungen* nach Art. 24 Abs. 1 i.V. m. Art. 25 und Art. 32 DSGVO und die Notwendigkeit bzw. Nicht-Notwendigkeit der Durchführung einer *Datenschutz-Folgenabschätzung* nach Art. 35 DSGVO können bei der jeweiligen Verarbeitung dokumentiert werden. In Fällen einer *Drittlandübermittlung* ist es auch sinnvoll zu dokumentieren, wie der Drittlandtransfer bei der konkreten Verarbeitung nach Art. 44 ff. DSGVO gerechtfertigt wird, ob der Drittlandtransfer also z. B. auf einen Angemessenheitsbeschluss oder andere geeignete Garantien, wie z. B. EU-Standardverträge, gestützt wird. Ein *Angemessenheitsbeschluss* ist ein Beschluss, der von der Europäischen Kommission gemäß Art. 45 DSGVO angenommen wird und durch den festgelegt wird, dass ein Drittland (d. h. ein Land, das nicht an die DSGVO gebunden ist) oder eine internationale Organisation ein angemessenes Schutzniveau für personenbezogene Daten bietet. Im Rahmen dieses Beschlusses werden die innerstaatlichen Rechtsvorschriften des Landes, seine Aufsichtsbehörden und die von ihm eingegangenen internationalen Verpflichtungen berücksichtigt.

Praxistipp: Beispiele für sinnvolle Ergänzungen des VVT

- Rechtsgrundlage der Verarbeitung
- Einsatz von Auftragsverarbeitern
- Risikoabschätzungen
- Hinweis auf Datenschutz-Folgenabschätzung
- Rechtfertigung einer Drittlandübermittlung (Angemessenheitsbeschluss oder geeignete Garantien)

Das VVT eines Auftragsverarbeiters

Den *Auftragsverarbeiter* trifft nach Art. 30 Abs. 2 DSGVO eine eigenständige Pflicht zur Führung eines Verarbeitungsverzeichnisses. Es muss jedoch nicht denselben Umfang wie das des Verantwortlichen haben, da der Auftragsverarbeiter auf Weisung des Verantwortlichen hin handelt. Zu beachten ist, dass der Auftragsverarbeiter in der Regel auch eigene Verarbeitungen vornimmt, bei denen er nicht Auftragsverarbeiter, sondern Verantwortlicher ist. So verarbeitet er in der Regel die personenbezogenen Daten seiner Beschäftigten als Verantwortlicher. Soweit er als Verantwortlicher tätig ist, muss er auch ein eigenes Verarbeitungsverzeichnis nach Art. 30 Abs. 1 DSGVO führen.

Nach Art. 30 Abs. 2 lit. a DSGVO hat der Auftragsverarbeiter in seinem Verarbeitungsverzeichnis den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten anzugeben. Anzugeben sind jeweils die konkreten Namen und Anschriften.

Art. 30 Abs. 2 lit. b DSGVO verlangt die Dokumentation der Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden. Dies können z. B. die Datenerhebung durch ein Callcenter, Hosting-Dienste (z. B. Bereitstellung von Webspace) oder die Datenträgerentsorgung sein.

Bei den Pflichten zur Dokumentation von Drittlandsachverhalten und der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO gemäß Art. 30 Abs. 2 lit. c und d DSGVO gilt nichts anderes als beim Verarbeitungsverzeichnis des Verantwortlichen.

5.1.5 Was passiert, wenn ich kein VVT führe bzw. es nicht pflege?

Welche *Sanktionen* drohen Ihrem Unternehmen eigentlich, wenn kein VVT aufgestellt und geführt wird? Wird der Aufsichtsbehörde auf deren Anfrage hin kein VVT vorgelegt oder wird es nicht ordnungsgemäß geführt, kann nach Art. 83 Abs. 4 lit. a DSGVO ein Bußgeld in Höhe von bis zu 10 Millionen EUR oder bis zu 2 % des gesamten weltweit erzielten Konzernjahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden. Die Aufsichtsbehörden können daneben viele weitere Maßnahmen ergreifen, die ihnen Art. 58 DSGVO einräumt.

Hinweis: Befugnisse der Aufsichtsbehörden nach Art. 58 DSGVO

- Anweisung, alle Informationen bereitzustellen, die für die Erfüllung der Aufgaben der Aufsichtsbehörden erforderlich sind
- Untersuchungen in Form von Datenschutzüberprüfungen durchführen
- Überprüfung der erteilten Zertifizierungen durchführen
- Hinweise auf vermeintliche Verstöße gegen die DSGO erteilen
- Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung der Aufgaben der Aufsichtsbehörden erforderlich sind, verlangen
- Zugang zu den Räumlichkeiten, einschließlich aller Datenverarbeitungsanlagen und -geräte, erhalten
- Warnung vor Datenschutzverstöße aussprechen
- Verwarnungen aussprechen
- Anweisungen zur Erfüllung von Betroffenenrechten erteilen
- Anweisungen zur Anpassung von Verarbeitungen an die DSGVO erteilen

- Anweisungen zur Information von Betroffenen bei Datenschutzverletzungen erteilen
- Beschränkungen und Verbote von Verarbeitungen vorübergehend und endgültig aussprechen
- Berichtigung, Löschung, Einschränkung anordnen
- Zertifizierungen widerrufen
- Geldbußen verhängen
- Aussetzung einer Drittlandübermittlung anordnen

Sie sehen, den Aufsichtsbehörden steht ein vielseitiges Instrumentarium zur Verfügung, um gegen Datenschutzverstöße vorzugehen.[11]

Dagegen haben Sie von *Mitbewerbern* und *Abmahnvereinen* wenig zu befürchten, da Datenschutzverstöße nach der derzeitigen Rechtsprechung nur dann abgemahnt werden können, wenn es sich bei den Datenschutzregelungen, gegen die verstoßen wird, um sogenannte Marktverhaltensregeln handelt. Die Rechenschaftspflichten, in die das VVT eingebettet ist, gehören nach derzeitiger Auffassung nicht dazu, sodass ein nicht oder nicht ordentlich geführtes VVT nicht abgemahnt werden kann.

Auch der Europäische Gerichtshof (EuGH) hat sich bereits mit dem VVT beschäftigt und entschieden, dass ein fehlendes oder unvollständiges VVT nicht dazu führt, dass eine Datenverarbeitung unrechtmäßig ist.[12]

5.2 Technische und organisatorische Maßnahmen (TOM) festlegen und dokumentieren

Verantwortliche und Auftragsverarbeiter sind nach Art. 32 Abs. 1 DSGVO verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko *angemessenes* Schutzniveau zu gewährleisten. Bei der Festlegung konkreter Maßnahmen sind der Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zweck der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeiten und Schweren des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.[13]

11 Siehe dazu auch Kapitel 10, »Folgen bei Datenschutzproblemen: Sanktionen, Abmahnungen und Schadenersatz«.

12 Siehe dazu EuGH, Urteil vom 04. Mai 2023 zum Az. C-60/22, online abrufbar unter *https://curia.europa.eu/juris/document/document.jsf?text=&docid=273289&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1* (zuletzt aufgerufen am 15. Juni 2023).

13 Siehe dazu Kapitel 3, »Technischer Datenschutz: Anforderungen der DSGVO an den IT-Betrieb«.

Die Vorschrift enthält keinen abschließenden Katalog von Maßnahmen, beschreibt aber beispielhaft einige Maßnahmen, die gegebenenfalls zu ergreifen sind und die im folgenden Kasten aufgezählt werden.

Praxistipp: Bereiche, die durch TOM nach Art. 32 DSGVO abgedeckt werden sollen

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Bei der Beurteilung der Angemessenheit des gewählten Schutzniveaus sind nach Art. 32 Abs. 2 DSGVO insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, vor allem durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Werden genehmigte Verhaltensregeln nach Art. 40 DSGVO oder genehmigte Zertifizierungsverfahren gemäß Art. 42 DSGVO eingehalten, kann dies nach Art. 32 Abs. 3 DSGVO als Faktor herangezogen werden, um die Erfüllung der Verpflichtungen aus Art. 32 Abs. 1 DSGVO nachzuweisen. Beides kommt derzeit in der Praxis kaum vor.

Schließlich schreibt Art. 32 Abs. 4 DSGVO vor, dass der Verantwortliche und der Auftragsverarbeiter Schritte unternehmen, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Eine ähnliche Vorschrift gab es bereits in § 9 BDSG alter Fassung. Zu dieser alten Norm gab es eine Anlage. Frühere TOM-Dokumentationen orientierten sich in Aufbau und Inhalt an dieser Anlage zu § 9 Satz 1 BDSG. Heute empfiehlt es sich, die Dokumentation sowohl formal als auch inhaltlich an Art. 32 DSGVO auszurichten. Eine einfache TOM-Dokumentation kann heute in etwa wie folgt aussehen:

Praxisbeispiel: TOM-Dokumentation nach Art. 32 DSGVO

1. Maßnahmen bzgl. der Datenschutzorganisation
   - DSB
   - Die Mitarbeiter wurden zur Vertraulichkeit verpflichtet.
   - Die Mitarbeiter werden regelmäßig zum Thema Datenschutz geschult.
   - Es gibt einen Workflow zur Erfüllung der Betroffenenrechte.
   - Es gibt eine Datenschutzrichtlinie.
2. Maßnahmen zur Sicherstellung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
   - Zutrittskontrolle

     Die Zugänge zu unserem Gebäude sind stets verschlossen.

     Besucher werden in Empfang genommen und beaufsichtigt.

     Das Gebäude/Gelände wird videoüberwacht.

     ...
   - Zugangskontrolle

     Unsere IT-Systeme sind passwortgeschützt.

     Es wird eine Zwei-Faktor-Authentifizierung eingesetzt.

     ...
   - Zugriffskontrolle

     Es gibt ein Berechtigungskonzept.

     Die Zugriffe werden protokolliert.

     ...
   - Trennungskontrolle

     Die eingesetzte Software ist mandantenfähig.

     ...
   - Pseudonymisierung

     Die Daten werden – soweit und sobald möglich – pseudonymisiert.

     ...
   - Datenträgerentsorgung/-vernichtung

     Die Datenträger werden durch einen Auftragsverarbeiter datenschutzgerecht vernichtet.

     Die Papierdokumente werden geschreddert.

     ...
3. Maßnahmen zur Sicherstellung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)
   - Weitergabekontrolle

     Die Daten werden stets verschlüsselt übertragen oder transportiert.

     ...

- Eingabekontrolle

  Die Eingaben werden protokolliert.

  Das eingesetzte Dokumentenmanagementsystem protokolliert Änderungen.

  ...

4. Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit (Art. 32. Abs. 1 lit. b DSGVO)
   - Verfügbarkeitskontrolle

     Es besteht ein Backup-Konzept.

     Es gibt eine unterbrechungsfreie Stromversorgung.

     Es werden eine Firewall und ein Anti-Maleware-Programm eingesetzt.

     ...
   - Rasche Wiederherstellbarkeit

     Es werden regelmäßig Rücksicherungen zwecks Feststellung der Funktionsfähigkeit des Backups durchgeführt.

     ...
5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)
   - Datenschutzmanagement

     Es gibt ein Datenschutzmanagement-System.

     ...
   - Datenschutzfreundliche Voreinstellungen (Privacy by Default)

     Die von uns verwendete Software wird mit datenschutzfreundlichen Voreinstellungen betrieben.

     Wir achten bei der Beschaffung von Software darauf, dass diese datenschutzfreundlich voreingestellt ist.

     ...
   - Datenschutz durch datenschutzfreundliche Technikgestaltung (Privacy by Design)

     Wir achten bei der Beschaffung von Software darauf, dass diese datenschutzfreundlich gestaltet ist.

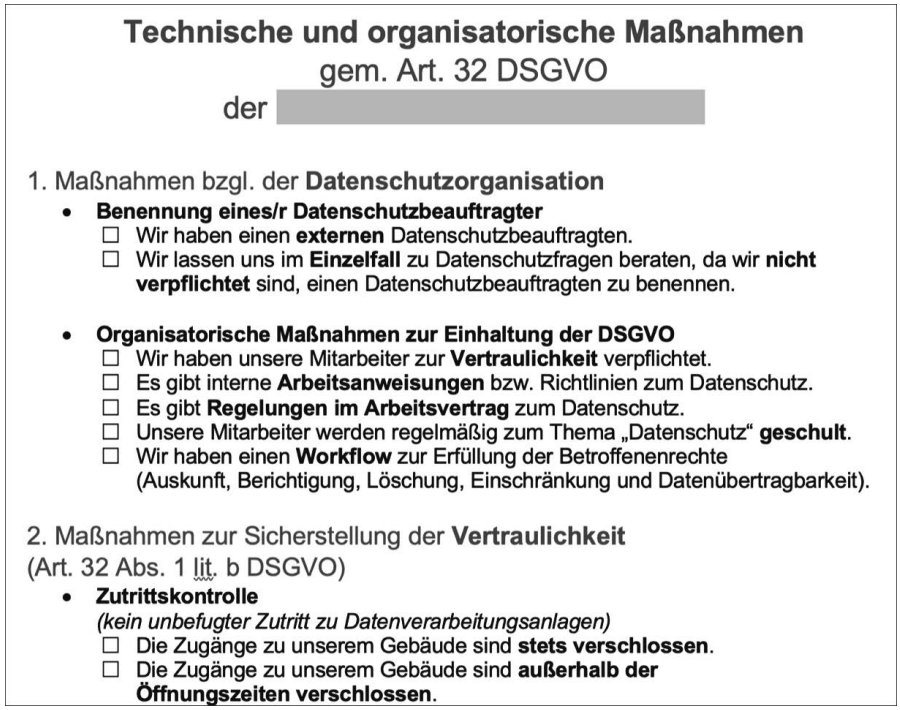
     Wenn wir Software entwickeln, wird diese datenschutzfreundlich gestaltet.

     ...
   - Auftragskontrolle

     Daten werden erst an Auftragsverarbeiter gegeben, wenn die Voraussetzungen von Art. 28 DSGVO erfüllt sind und insbesondere ein Auftragsverarbeitungsvertrag geschlossen wurde.

     ...

Die TOM-Dokumentation erfolgt meist in einem gesonderten Dokument. Ähnlich wie beim VVT sind Sie bei der Wahl der Mittel frei. Sie können Ihre TOM in einem Word- oder Excel-Dokument dokumentieren oder eine spezielle Software einsetzen (siehe dazu Abbildung 5.3). Sind Sie Auftragsverarbeiter, gehört die TOM-Dokumentation immer als Anlage zum Auftragsverarbeitungsvertrag (AVV).



Technische und organisatorische Maßnahmen
gem. Art. 32 DSGVO
der

1. Maßnahmen bzgl. der **Datenschutzorganisation**
   - **Benennung eines/r Datenschutzbeauftragter**
     - ☐ Wir haben einen **externen** Datenschutzbeauftragten.
     - ☐ Wir lassen uns im **Einzelfall** zu Datenschutzfragen beraten, da wir **nicht verpflichtet** sind, einen Datenschutzbeauftragten zu benennen.
   - **Organisatorische Maßnahmen zur Einhaltung der DSGVO**
     - ☐ Wir haben unsere Mitarbeiter zur **Vertraulichkeit** verpflichtet.
     - ☐ Es gibt interne **Arbeitsanweisungen** bzw. Richtlinien zum Datenschutz.
     - ☐ Es gibt **Regelungen im Arbeitsvertrag** zum Datenschutz.
     - ☐ Unsere Mitarbeiter werden regelmäßig zum Thema „Datenschutz" **geschult**.
     - ☐ Wir haben einen **Workflow** zur Erfüllung der Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit).

2. Maßnahmen zur Sicherstellung der **Vertraulichkeit** (Art. 32 Abs. 1 lit. b DSGVO)
   - **Zutrittskontrolle**
     (kein unbefugter Zutritt zu Datenverarbeitungsanlagen)
     - ☐ Die Zugänge zu unserem Gebäude sind **stets verschlossen**.
     - ☐ Die Zugänge zu unserem Gebäude sind **außerhalb der Öffnungszeiten verschlossen**.

Abbildung 5.3 Ausschnitt aus einer TOM-Dokumentation

5.3 Richtig informieren: Datenschutzhinweise für Betroffene

Vermutlich haben Sie in den letzten Jahren zahllose *Datenschutzhinweise* erhalten und sich dabei vielleicht gefragt, ob das wirklich so sein muss. Die Antwort lautet: Leider ja. Die DSGVO hat die *Informationspflichten* deutlich erweitert. Sie werden von Unternehmen häufig als Belastung empfunden, stellen aber einen zentralen Bestandteil der Betroffenenrechte dar.

5.3.1 Transparenzgrundsatz

Die Informationspflichten finden ihre Grundlage im Grundsatz der Transparenz. Der *Transparenzgrundsatz* wurzelt wiederum letztlich in der Grundrechtecharta der Europäischen Union. Höher kann man ein Recht innerhalb der EU gar nicht aufhän-

gen. Im deutschen Recht ist der Transparenzgrundsatz Teil des Grundrechts auf informationelle Selbstbestimmung, das aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (GG) hergeleitet wird.

Hinweis: Das Volkszählungsurteil des Bundesverfassungsgerichts

Bereits im Jahre 1983 hat das Bundesverfassungsgericht in seinem berühmten *Volkszählungsurteil*[14] geurteilt:

Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.

Für den Verantwortlichen ergeben sich aus dem Transparenzgrundsatz zahlreiche Pflichten, insbesondere Informationspflichten. Die beiden prominentesten Informationspflichten finden Sie in Art. 13, 14 DSGVO, wobei Art. 13 DSGVO Informationspflichten für den Fall aufstellt, dass die Erhebung der personenbezogenen Daten bei der betroffenen Person selbst erfolgt, und Art. 14 DSGVO den Fall regelt, dass die personenbezogenen Daten nicht direkt beim Betroffenen erhoben werden. Der früher im BDSG a. F. vorhandene *Grundsatz der Direkterhebung*, nachdem die Daten grundsätzlich beim Betroffenen zu erheben waren, findet sich in der DSGVO nicht mehr. Dafür ist die Informationserteilung als Bringschuld ausgestaltet. Der Verantwortliche muss die Informationen ohne Nachfrage des Betroffenen zur Verfügung stellen, und es kann selbst durch ein Vertrag zwischen dem Betroffenen und dem Verantwortlichen nicht auf die Erteilung der Informationen verzichtet werden.

5.3.2 Allgemeine Regeln zu Betroffenenrechten in Art. 12 DSGVO

Die Art. 13 und 14 DSGVO müssen Sie immer zusammen mit Art. 12 DSGVO lesen. Dort sind einige Vorgaben enthalten, die für alle folgenden Betroffenenrechte gelten. Im Hinblick auf die Informationspflichten finden sich hier Anforderungen an die Form sowie die inhaltliche Gestaltung und Fristen. Die Informationen müssen nach Art. 12 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt werden. Sie müssen schriftlich, gegebenenfalls auch elektronisch oder in anderer Form erteilt werden. Die mündliche Erteilung ist damit zwar zulässig aber nicht zu empfehlen, weil der Verantwortliche im Zweifel nachweisen muss, dass er die Informationen erteilt hat.

14 Siehe dazu BVerfG, Urteil vom 15. Dezember 1983 (Az. BvR 209/83), online abrufbar unter *www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html* (zuletzt aufgerufen am 15. Juni 2023).

Umstritten ist derzeit noch, ob bei der Erteilung der Informationen ein *Medienbruch* zulässig ist. Ein Medienbruch liegt z. B. vor, wenn Sie in einem Brief auf weitergehende Informationen auf einer Internetseite verweisen (per Angabe einer URL oder per QR-Code). In bestimmten Situationen wird man kaum ohne Medienbruch auskommen. Beim Telefongeschäft wird man z. B. kaum erst einmal die Datenschutzinformationen komplett vorlesen müssen. IoT-Geräte haben möglicherweise kein oder kein ausreichend großes Display, um sämtliche Informationen anzuzeigen. In allen Fällen sollten Sie darauf achten, dass ein leicht erkennbarer und erreichbarer Verweis auf die vollständigen Datenschutzinformationen angebracht ist, beispielsweise in Form eines Links.

Nicht vorgeschrieben und für die Rechtmäßigkeit der Verarbeitung ohne Bedeutung ist die tatsächliche Wahrnehmung der angebotenen Informationen durch den Betroffenen. Der Betroffene muss lediglich die Möglichkeit zur Kenntnisnahme haben. Ob er davon Gebrauch macht oder nicht, ist seine Sache.

Sie sollten deshalb Formulierungen vermeiden, die auf eine vertragliche Vereinbarung oder die Einbeziehung der Datenschutzhinweise in einen Vertrag hindeuten. Es sollte also möglichst nicht formuliert werden, dass der Betroffene mit den Datenschutzhinweisen »einverstanden« ist oder diese »akzeptiert«. Bei online zur Verfügung gestellten Datenschutzhinweisen sollten Sie keine Checkboxen oder Ähnliches verwenden, die die Betroffenen zunächst aktivieren müssen. Es reicht der schlichte Hinweis darauf, wo der Betroffene die Informationen finden kann. Aus diesem Grund gehören Datenschutzhinweise auch nicht in die *Allgemeinen Geschäftsbedingungen (AGB*).

Eine besondere Form der Informationserteilung ermöglicht Art. 12 Abs. 7 DSGVO, nach dem die Informationen auch durch standardisierte *Bildsymbole* erteilt werden können (siehe dazu Abbildung 5.4). Die Verwendung von Bildsymbolen ist nicht verpflichtend und hat sich bislang noch nicht durchgesetzt. Gänzlich ersetzen können Bildsymbole die Informationen nicht. Im Parlamentsentwurf zur DSGVO waren sechs Beispiele für Mustersymbole enthalten, die wir hier wiedergeben, damit Sie eine Vorstellung von derartigen Bildsymbolen bekommen.

Bei der Erstellung von Datenschutzhinweisen sollte man sich immer wieder daran erinnern, dass diese in *klarer und einfacher Sprache* verfasst werden müssen und sich in aller Regel an Laien und nicht an Datenschutzexperten richten. Diese Grundregel wird sehr häufig missachtet, und man sieht bei vielen Datenschutzhinweisen häufig schon wegen der schieren Masse an Text den sprichwörtlichen Wald vor lauter Bäumen nicht mehr. Besonders häufig kranken ausschweifende Datenschutzerklärungen auf Websites an diesem Problem.

Abbildung 5.4 Beispiele für standardisierte Bildsymbole (Quelle: www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/01/EU-DSGVO-Entwurf-nach-EU-Parlament-22.11.2013-.pdf)

Ein praktisches Problem ergibt sich daraus, dass komplexe Verarbeitungsvorgänge nur schwer in wenigen leicht verständlichen Worten beschrieben werden können. Ein Zuviel an Informationen kann leicht zur Intransparenz führen. Das ist ein kaum lösbarer Zielkonflikt zwischen vollständiger und trotzdem transparenter Information. Präzision und Vollständigkeit stehen teilweise im Widerspruch zu Klarheit und Einfachheit. Zur Lösung des Spannungsverhältnisses zwischen Verständlichkeit und Vollständigkeit der Information wird ein *Zwei-Stufen-Modell* vorgeschlagenen, wonach dem Betroffenen auf der ersten Stufe zunächst eine knapp gehaltene Information übermittelt wird, die ihn in groben Zügen über die Verarbeitung informiert, und auf der zweiten Stufe die vollständigen Informationen mittels eines Verweises zur Verfü-

gung gestellt werden. Solche gestaffelten Informationen bieten sich vor allem bei komplexen Datenverarbeitungsvorgängen an, die im Internet erläutert werden können, da dort die verschiedenen Ebenen der Informationen leicht verlinkt werden können. In jedem Fall setzt die geforderte Verständlichkeit bei längeren Texten eine sinnvolle Ordnung und eine Untergliederung mittels aussagekräftiger Überschriften voraus.

Von großer praktischer Relevanz ist die Frage, in welcher *Sprache* die Informationen zur Verfügung gestellt werden müssen. Eine ausdrückliche Regelung dazu fehlt in der DSGVO. Das Marktortprinzip von Art. 3 Abs. 2 DSGVO spricht allerdings dafür, dass der Verantwortliche die Informationen und Auskünfte in der Sprache der hauptsächlich adressierten Personen erteilen muss. Richtet ein in den USA ansässiges Unternehmen beispielsweise einen Internetshop in deutscher Sprache unter einer .de-Domain ein, muss die Datenschutzerklärung in deutscher Sprache vorgehalten werden. Das Gleiche dürfte auch gelten, wenn das Unternehmen seinen Sitz in Spanien hat, sich mit seinem Internetshop aber erkennbar (Kriterien sind u. a. Sprache und Domain) an ein deutschsprachiges Publikum richtet.

5.3.3 Datenschutzhinweise nach Art. 13 DSGVO

Art. 13 DSGVO dürfte die in der Praxis am häufigsten zur Anwendung kommende Vorschrift zur Erteilung von Informationen an Betroffene sein. Sie regelt den Standardfall der Erhebung personenbezogener Daten direkt beim Betroffenen, während Art. 14 DSGVO den Fall regelt, dass die Daten ohne Beteiligung des Betroffenen bei einem Dritten erhoben werden.

Innerhalb von Art. 13 DSGVO ist zwischen den vier Absätzen zu differenzieren: Die Abs. 1 und 2 regeln den Inhalt der zu erteilenden Informationen bei der erstmaligen Datenverarbeitung, Abs. 3 regelt den Fall der Zweckänderung, und Abs. 4 sieht Ausnahmen vor.

Informationen nach Art. 13 Abs. 1 DSGVO

Die Informationspflichten nach Art. 13 DSGVO werden durch das *Erheben* personenbezogener Daten bei der betroffenen Person ausgelöst. Die Erhebung ist nach Art. 4 Nr. 2 DSGVO eine Phase der Verarbeitung. Demnach ist unter Erhebung ein Vorgang zu verstehen, bei dem sich die erhebende Stelle Daten über eine betroffene Person beschafft oder Kenntnis von den Daten erlangt. Erforderlich ist ein aktives Handeln des Verantwortlichen. Ob die Daten automatisiert (z. B. durch Sensoren, Videokameras o. Ä.) oder zunächst manuell erhoben werden, ist nicht relevant. Es reicht auch aus, wenn die Daten zunächst von einem Menschen wahrgenommen und von diesem dann in ein IT-System übertragen werden. Schreiben Sie also den Namen und die Kontaktdaten von einer Visitenkarte in Ihr CRM-System ab, erheben Sie die Daten.

Die Informationen sind im Zeitpunkt der Erhebung zu erteilen, also umgehend, nachdem mit der Verarbeitung begonnen worden ist. Erfolgt die Erhebung auf Initiative des Betroffenen hin, bevor die Möglichkeit der Information besteht (also z. B. bei einer Initiativbewerbung oder einer Beschwerde), sind die Informationen schnellstmöglich zu erteilen, also z. B. im Rahmen einer Eingangsbestätigungs-E-Mail. Kommt es später zu Änderungen bei der Verarbeitung, die sich auf den Inhalt der Informationen auswirken, sind die geänderten Informationen dem Betroffenen frühzeitig vor der Änderung zur Verfügung zu stellen, damit dieser gegebenenfalls rechtzeitig Einwände vorbringen kann oder eines seine Rechte geltend machen kann (z. B. Widerruf einer Einwilligung).

Praxistipp: Nach Art. 13 Abs. 1 DSGVO sind mitzuteilen

- Name und Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die Rechtsgrundlage für die Verarbeitung
- die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden, wenn die Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO beruht
- gegebenenfalls Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, und zugleich die Information, ob ein Angemessenheitsbeschluss der Kommission vorhanden ist oder nicht (bei Fehlen eines solchen Beschlusses ist auf geeignete oder angemessene Garantien zu verweisen und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.)

Nach Art. 13 Abs. 1 lit. a DSGVO sind der *Name und die Kontaktdaten des Verantwortlichen* sowie gegebenenfalls seines Vertreters anzugeben. Welche Kontaktdaten das im Einzelnen sind, ist in der DSGVO nicht geregelt. Nach dem Sinn und Zweck der Informationspflicht soll dem Betroffenen die Kontaktaufnahme ermöglicht und erleichtert werden, sodass Kontaktmöglichkeiten über verschiedene Kanäle angegeben werden sollten. Dazu gehört sicher der vollständige Name; bei natürlichen Personen also mindestens ein Vorname und der Nachname, bei Kaufleuten, Personengesellschaften oder juristischen Personen die vollständige Firmierung inklusive Rechtsformzusatz, die postalische Anschrift im Sinne einer ladungsfähigen Anschrift (Postfach reicht nicht), eine Telefonnummer und eine E-Mail-Adresse. Mit *Vertreter* ist übrigens – wie bereits oben beim VVT erläutert – nicht der gesetzliche oder organschaftliche Vertreter, also z. B. der Geschäftsführer einer GmbH, gemeint, sondern ein Vertreter im Sinne von Art. 27 DSGVO, also der Vertreter von nicht in der EU niedergelassenen Verantwortlichen. Den Fall werden Sie in der Regel nicht haben.

Wenn ein *Datenschutzbeauftragter* benannt ist, müssen dessen *Kontaktdaten* angegeben werden. Im Unterschied zur Angabe im Verarbeitungsverzeichnis ist hier die Angabe des konkreten Namens des DSB nicht erforderlich. Wenn Sie Ihre Datenschutzinformationen nicht immer ändern wollen, wenn Sie den DSB wechseln, verwenden Sie als Kontaktmöglichkeit einfach eine E-Mail-Adresse nach dem Muster *datenschutz@example.com*. Ist kein Datenschutzbeauftragter benannt, kann die Angabe ersatzlos entfallen. Es ist nicht über die Gründe aufzuklären, warum kein DSB benannt ist.

Nach Art. 13 Abs. 1 lit. c DSGVO sind die *Zwecke*, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die *Rechtsgrundlagen* für die Verarbeitung anzugeben. Mitzuteilen sind alle Zwecke, die der Verantwortliche zum Zeitpunkt der Erhebung verfolgt, wobei nur die konkret in Erwägung gezogenen Zwecke und nicht alle erdenklichen Zwecke auf Vorrat genannt werden dürfen. Zwecke können allgemein gehalten werden (z. B. Vertragsabwicklung, Lohnabrechnung, Marketing usw.), dürfen aber nicht völlig unspezifisch (z. B. Big Data) angegeben werden. Die Angabe der Rechtsgrundlage ist wichtig, damit der Betroffene die Rechtmäßigkeit der Verarbeitung zu dem angegebenen Zweck prüfen kann. Außerdem haben Sie an dieser Stelle auch selbst noch einmal die Möglichkeit, für sich zu prüfen, ob es für die Verarbeitung, über die Sie informieren, auch wirklich eine tragfähige Rechtsgrundlage gibt.

Beruht die Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO, sind nach Art. 13 Abs. 1 lit. d DSGVO die *berechtigten Interessen*, die von dem Verantwortlichen oder Dritten verfolgt werden, anzugeben. Ausreichend ist die Angabe der verfolgten Interessen; nicht zwingend angegeben werden muss das Ergebnis der durchgeführten Interessenabwägung, bei der die vom Verantwortlichen verfolgten Interessen mit den Interessen, Grundrechten und Grundfreiheiten des Betroffenen abgewogen werden.

Nach Art. 13 Abs. 1 lit. e DSGVO sind gegebenenfalls die *Empfänger* oder Kategorien von Empfängern der personenbezogenen Daten anzugeben. Ob interne Übermittlungen innerhalb des Verantwortlichen (z. B. Personalabteilung an Rechtsabteilung) mitgeteilt werden müssen, ist umstritten. Sicherheitshalber sollten im Zweifel auch interne Empfänger bzw. Empfängerkategorien angegeben werden. Demgegenüber sind die Auftragsverarbeiter sicher Empfänger und deshalb anzugeben. Umstritten ist, ob die Empfänger – sofern zum Zeitpunkt der Informationserteilung bekannt – namentlich benannt werden müssen oder ob die Nennung einer Branchenbezeichnung bzw. die Umschreibung in abstrakter Form ausreichend ist (z. B. Versandunternehmen, Konzernunternehmen, Newsletter-Dienstleister usw.). Für eine namentliche Nennung spricht die größtmögliche Transparenz. Für die Wahlmöglichkeit des Verantwortlichen spricht der Wortlaut der Vorschrift, der ein Alternativverhältnis beschreibt. Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen geht in ihrem 26. Bericht zum Datenschutz auf Seite 98 f. davon aus, dass die bloße Nennung von Kategorien von Empfängern *nur dann hinnehmbar ist, wenn die Zahl der Empfänger*

sehr groß oder nur schwer recherchierbar ist oder ein berechtigtes Geheimhaltungsinteresse der Preisgabe konkreter Empfänger entgegensteht.[15] Der EuGH hat im Rahmen eines Verfahrens über einen Auskunftsanspruch nach Art. 15 DSGVO entschieden, dass im Rahmen einer Auskunft die konkreten Empfänger namentlich genannt werden müssen und die Angabe bloßer Kategorien nicht ausreichend ist.[16] Der Wortlaut von Art. 15 Abs. 1 lit. c DSGVO lässt – wie Art. 13 Abs. 1 lit. e DSGVO – die Nennung von Empfängern oder Kategorien von Empfängern zu. Allerdings legt der EuGH den Wortlaut im Lichte der übrigen Betroffenenrechte dahingehend aus, dass der Verantwortliche grundsätzlich die Identität der Empfänger offenlegen müsse, damit der Betroffene weitere Betroffenenrechte effektiv ausüben können. Ausnahmen gibt es nur für den Fall, das der Verantwortliche keine konkreten Empfänger identifizieren kann. Ob die Entscheidung wegen des vergleichbaren Wortlauts der Normen auch auf Art. 13 Abs. 1 lit. e DSGVO zu übertragen ist und deshalb auch im Rahmen von Datenschutzhinweisen – soweit möglich – konkrete Empfänger benannt werden müssen, ist derzeit noch umstritten. Die meisten bisher veröffentlichten Stimmen gehen davon aus, dass die Entscheidung nicht übertragbar ist, weil bereits der Generalanwalt in seinen dem Urteil vorangehenden Schlussanträgen klargestellt hat, dass die Informationspflichten einer anderen Logik unterliegen als das Auskunftsrecht. Die Informationspflichten müssen zu Beginn der Verarbeitung erfüllt werden. Zu diesem Zeitpunkt stehen die konkreten Empfänger manchmal noch gar nicht fest. Der Betroffene wird durch die Angabe der Kategorien auch nicht in der Durchsetzung seiner Rechte beschränkt. Über einen Auskunftsanspruch kann er vollständige Transparenz herstellen.

Schließlich ist nach Art. 13 Abs. 1 lit. f DSGVO gegebenenfalls über die Absicht des Verantwortlichen zu informieren, die personenbezogenen Daten an ein *Drittland* oder an eine internationale Organisation zu übermitteln. Gemeint ist nicht nur die Übermittlung an anderes Land, sondern auch die Übermittlung an einen in einem Drittland ansässigen Empfänger. Darüber hinaus ist auch über das Vorliegen oder Fehlen eines Angemessenheitsbeschlusses zu informieren. Soll die Übermittlung auf andere geeignete Garantien, verbindliche interne Datenschutzvorschriften (Binding Corporate Rules – BCR) oder eine Ausnahme nach Art. 49 DSGVO gestützt werden, muss der Betroffene darüber informiert werden, um welche geeigneten oder angemessenen Garantien es sich handelt. Der Betroffene muss auch darüber aufgeklärt werden, wo entweder eine Kopie des Angemessenheitsbeschlusses oder der Garantien zu erhalten ist oder diese Dokumente sonst verfügbar sind. An dieser Stelle wird es meist schwierig, sodass im Fall von Drittlandübermittlungen in der Regel ein Datenschutzexperte befragt werden sollte.

15 Der 26. Bericht der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW ist abrufbar unter *www.ldi.nrw.de/berichte* (zuletzt aufgerufen am 15. Juni 2023).

16 Siehe dazu EuGH, Urteil vom 12. Januar 2023 (Az. C-154/21), online abrufbar unter *https://curia.europa.eu/juris/document/document.jsf?text=&docid=269146&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=992652* (zuletzt aufgerufen am 15. Juni 2023).

Informationen nach Art. 13 Abs. 2 DSGVO

Neben den Informationen aus Abs. 1 sind in der Regel auch sämtliche Informationen aus Abs. 2 zu erteilen (siehe Abbildung 5.5).

Informationen zur Verarbeitung personenbezogener Daten

Wir sind nach der EU-Datenschutzgrundverordnung (DSGVO) verpflichtet, Sie über die Verarbeitung Ihrer personenbezogenen Daten zu informieren. Dieser Informationspflicht kommen wir durch die Übergabe dieser Datenschutzinformationen nach.

Name und Kontaktdaten des für die Verarbeitung Verantwortlichen

Muster GmbH, Musterstraße 1, 1245 Musterstadt, info@example.com, Tel. 01234/ 12345678

Kontaktdaten des Datenschutzbeauftragten

Unseren Datenschutzbeauftragten erreichen Sie unter unserer Anschrift mit dem Zusatz – Datenschutzbeauftragter – oder unter datenschutz@example.com.

Zweck und Rechtsgrundlage der Verarbeitung

Die Verarbeitung Ihrer Daten erfolgt, zur Vertragsanbahnung/Vertragserfüllung gem. Art. 6 Abs. 1 S. 1 lit. b DSGVO und zur Information/Werbung für eigene Zwecke gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO.

Speicherdauer bzw. Kriterien für die Festlegung der Speicherdauer

Die für von uns erhobenen personenbezogenen Daten werden so lange wie erforderlich gespeichert und dann gelöscht, wenn wir nicht gesetzlich, z. B. auf Grund von steuer- und handelsrechtlichen Aufbewahrungs- und Dokumentationspflichten (aus HGB oder AO), zu einer längeren Speicherung verpflichtet sind. Die gesetzliche Aufbewahrungsfrist für Handelsbriefe beträgt z. B. 6 Jahre, für steuerrelevante Unterlagen 10 Jahre.

Weitergabe Ihrer Daten

Wir geben Ihre Daten nur an Auftragsverarbeiter weiter.

Übermittlung Ihrer Daten

Wir übermitteln Ihre Daten nicht an ein Drittland oder eine internationale Organisation.

Automatisierte Entscheidungsfindung einschließlich Profiling

Ihre Daten werden keiner automatisierten Entscheidungsfindung einschließlich Profiling unterworfen.

Bereitstellung von Daten

Wenn Sie uns die für die Vertragserfüllung erforderlichen Daten nicht zur Verfügung stellen, können wir keinen Vertrag mit Ihnen abschließen.

Betroffenenrechte

Sie haben das Recht:

- Auskunft zu verlangen
- Berichtigung zu verlangen
- Löschung zu verlangen
- Einschränkung der Verarbeitung zu verlangen
- auf Datenübertragbarkeit
- sich bei einer Aufsichtsbehörde zu beschweren
- Widerspruch gegen eine Verarbeitung einzulegen, die auf Grundlage von berechtigten Interessen erfolgt
- eine uns etwa erteilte Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird

Abbildung 5.5 Beispiel für Datenschutzhinweise nach Art. 13 DSGVO

Praxistipp: Nach Art. 13 Abs. 2 DSGVO sind mitzuteilen

- Speicherdauer
- Betroffenenrechte
- Belehrung über Widerrufsrecht bei einer Einwilligung
- Beschwerderecht bei einer Aufsichtsbehörde
- Pflicht zur Bereitstellung der Daten
- automatisierte Entscheidungsfindung einschließlich Profiling

Die *Speicherdauer* ist – wenn möglich – konkret in Tagen, Monaten oder Jahren anzugeben. Steht die Speicherdauer zum Zeitpunkt der Erhebung der Daten noch nicht fest, sind Kriterien zur Bestimmung der Speicherdauer anzugeben. Vorsichtig sollten Sie – wie auch im VVT – ebenso an dieser Stelle mit ganz allgemeinen Beschreibungen wie z. B. »Wir löschen Ihre Daten, wenn der oben genannte Zweck erreicht ist und kein gesetzlichen Aufbewahrungsfristen mehr bestehen.« sein. Zumindest die gesetzlichen Aufbewahrungsfristen lassen sich in der Regel konkret bestimmen und dann auch konkret benennen. Wer ein Löschkonzept hat, profitiert auch an dieser Stelle davon, weil er die Löschfristen daraus entnehmen kann.

Ganz wichtig ist die Information über die *Betroffenenrechte*. Diese müssen zumindest aufgezählt werden. Ob man zu jedem Betroffenenrecht auch den passenden Artikel nennt und auch noch eine kurze Beschreibung hinzufügt, ist Geschmackssache. Zu lange Texte sollten allerdings vermieden werden, weil die Belehrung über die Betroffenenrechte sonst sehr lang, unübersichtlich und damit intransparent werden kann.

Praxistipp: Betroffenenrechte über die zu Informieren ist

- Auskunft (Art. 15 DSGVO)
- Berichtigung (Art. 16 DSGVO)
- Löschung (Art. 17 DSGVO)
- Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Widerspruch (Art. 21 DSGVO)
- Datenübertragbarkeit (Art. 20 DSGVO)
- Beschwerderecht bei einer Aufsichtsbehörde

Nach Art. 13 Abs. 2 lit. e DSGVO ist darüber zu informieren,

1. ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsschluss erforderlich ist,
2. ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen
3. welche möglichen Folgen die Nichtbereitstellung hätte