



Gesellschaft für Datenschutz  
und Datensicherheit e.V.

# GDD-Praxishilfe DS-GVO

Verzeichnis von Verarbeitungstätigkeiten –  
Verantwortlicher



<b>Vorwort .....</b>	<b>3</b>
<b>1. Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche .....</b>	<b>4</b>
1.1 Ausgangspunkt DS-GVO .....	4
1.2 Zweck .....	4
1.3 Terminologie: VVT im engeren und im weiteren Sinne .....	5
1.4 Verpflichtete .....	5
1.5 Führung des VVT durch Vertreter in der EU .....	6
1.6 Formalien .....	6
1.7 Inhalte .....	7
<b>2. Muster von Aufsichtsbehörden .....</b>	<b>8</b>
<b>3. Organisation des VVT .....</b>	<b>9</b>
3.1 Prämissen .....	9
3.2 Rollen .....	9
3.3 Beispiel zur Gliederung / zum Aufbau einer Policy zum VVT .....	12
3.3.1 Zielsetzungen der Policy .....	12
3.3.2 Integration der Policy im Unternehmen .....	12
3.3.3 Policy regelt: Verantwortlichkeit im Unternehmen .....	13
3.3.4 Policy legt fest: Vorlage zum Erstellen eines VVT .....	13
3.3.5 Policy legt fest: Meldung einer Verarbeitung erfolgt durch/mittels .....	13
3.3.6 Policy regelt: regelmäßige Kontrolle der Verarbeitungen und des VVT .....	14
3.3.7 Policy legt fest: wer kommuniziert mit der Aufsichtsbehörde .....	14
3.3.8 Checkliste Policy VVT .....	15
<b>4. Der DSB im Kontext des VVT .....</b>	<b>15</b>
<b>5. Anlage Muster für ein VVT .....</b>	<b>16</b>
5.1 Muster Vorblatt für ein VVT .....	18
5.2 Muster Hauptblatt für ein VVT für Angaben zu den einzelnen Verarbeitungstätigkeiten .....	20
<b>6. Anlage Muster für eine Verarbeitungsmeldung .....</b>	<b>25</b>
<b>7. Anlage Muster zum VVT von EU-Aufsichtsbehörden .....</b>	<b>37</b>

# Verzeichnis von Verarbeitungstätigkeiten – Verantwortlicher

Die erste Auflage dieser Praxishilfe wurde in der Zeit vor dem Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) verfasst. Im Vordergrund stand der Übergang vom Instrumentarium des Bundesdatenschutzgesetzes in der bis zum 25. Mai 2018 geltenden Fassung (BDSG a.F.) zu den Anforderungen der DS-GVO.

Seit der Veröffentlichung der ersten Auflage haben viele Unternehmen Erfahrungen mit der Organisation des Verzeichnisses von Verarbeitungstätigkeiten (VVT) gewonnen. So kamen die ersten Querschnittprüfungen der Datenschutzaufsichtsbehörden durch die LFD-Niedersachsen und das LDA-Bayern im Jahr 2018 im Rahmen von Fragebogenaktionen zu dem Ergebnis, dass die befragten Unternehmen im Bereich der VVTs „überwiegend gut aufgestellt“ waren.

Auch haben seitdem weitere Verbände und auch einige Aufsichtsbehörden in der EU Hilfestellungen und Musterverzeichnisse für Unternehmen und Behörden zur Verfügung gestellt.

Die vorliegende Neubearbeitung der Praxishilfe soll nach wie vor die Begriffe und Grundlagen des VVT erläutern. Dabei liegt der Schwerpunkt auf der praktischen Umsetzbarkeit für Unternehmen jeglicher Größe.

In Auseinandersetzung mit den publizierten Beispielen der Aufsichtsbehörden werden Muster für ein VVT und für die hierzu erforderlichen Verarbeitungsmeldungen entwickelt und erläutert.

Außerdem werden Empfehlungen für die Organisation des VVT im Unternehmen gegeben: Wer erfasst die erforderlichen Informationen, sammelt, pflegt und aktualisiert sie und wie kann dieser Prozess im Rahmen einer „Policy zum VVT“ geregelt werden?

**Für den fachlichen Rat bei der Erstellung dieser Praxishilfe dankt die GDD:**

**>> Michael Gutjahr**

*Referent Datenschutz, innogy SE*

**>> Stefan Hardelt**

*Unternehmensberatung Datenschutz*

**>> Rechtsanwalt Berthold Meyer**

**>> Rechtsanwalt Thomas Mütthlein**

*DMC Datenschutz Management + Consulting GmbH + Co KG,  
GDD-Vorstand*

**>> Dirk Niedernhöfer**

*Geschäftsführer adreko GmbH /  
externer Datenschutzbeauftragter*

# 1. Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche

## 1.1 Ausgangspunkt DS-GVO

Nach Art. 30 Abs. 1 DS-GVO muss jeder Verantwortliche ein „Verzeichnis von Verarbeitungstätigkeiten“ (im Folgenden abgekürzt: „VVT“) führen.

Das Verzeichnis enthält

- >> einige allgemeine Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit a DS-GVO),
- >> eine Auflistung aller „Verarbeitungen“ (Art. 4 Ziff. 2 DS-GVO), die in seinem Zuständigkeitsbereich liegen,
- >> mit spezifischen Angaben zu den einzelnen Verarbeitungstätigkeiten (Zwecke, Datenkategorien, Betroffenenkategorien, Empfänger, Drittlandübermittlungen, Löschrufen, technisch/organisatorische Maßnahmen Art. 30 Abs. 1 lit b – g DS-GVO).

## 1.2 Zweck

Das VVT dient hauptsächlich zum Nachweis der Einhaltung der DS-GVO (Erwägungsgrund 82 DS-GVO) und ist damit ein Instrument der „Rechenschaftspflicht“ (Art. 5 Abs. 2 DS-GVO). Es ist auf Anfrage der Aufsichtsbehörde vorzulegen, damit die Behörde die Verarbeitungsvorgänge anhand des Verzeichnisses kontrollieren kann (Art. 30 Abs. 4 DS-GVO; Erwägungsgrund 82 DS-GVO).

Die Rechenschaftspflicht des Verantwortlichen im Sinne von Art. 5 Abs. 2 DS-GVO ist umfassend und legt ihm die Verpflichtung auf, alle Grundsätze des Art. 5 Abs. 1 DS-GVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit) einzuhalten und die Einhaltung dieser Grundsätze nachzuweisen.

Der Nachweis im Rahmen des notwendigen Datenschutz-Managements erfordert also die systema-

tische betriebsinterne Erfassung von deutlich mehr Angaben und Informationen als in Art. 30 Abs. 1 DS-GVO für das VVT vorgeschrieben wird. Zum Beispiel auch das Vorhandensein von Einwilligungen (Art. 7 Abs. 1 DS-GVO), die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1 DS-GVO) und das Ergebnis von Datenschutz-Folgenabschätzungen (Art. 35 Abs. 7 DS-GVO) muss der Verantwortliche durch entsprechende Dokumentationen nachweisen können.

Die deutschen Aufsichtsbehörden sehen das VVT als zentralen Bestandteil der Dokumentation und als „Herzstück jedes Datenschutzkonzeptes“<sup>1</sup>, mit dem insbesondere auch zusätzlich:

- >> die Festlegung der Verarbeitungszwecke nach Art. 5 Abs. 1 lit. b DS-GVO,
- >> die geeigneten technischen und organisatorischen Maßnahmen nach Art. 24 Abs. 1 und Art. 32 DS-GVO,
- >> die Notwendigkeit und die Durchführung von Datenschutzfolgenabschätzung nach Art. 35 DS-GVO

dokumentiert werden können und gehen damit über die Anforderungen des Art. 30 Abs. 1 DS-GVO hinaus.

Ohne eine umfassende und strukturierte Dokumentation dürften auch die Beratungs- und Überwachungspflichten des Datenschutzbeauftragten (im Folgenden: „DSB“) nach Art. 39 DS-GVO kaum umsetzbar sein.

Allerdings sollten sowohl terminologisch als auch inhaltlich:

- >> die Erfüllung der speziellen Dokumentationspflichten aus Art. 30 Abs. 1 DS-GVO
- >> und die Funktion eines solchen Verzeichnisses als Strukturelement für die Erfassung weiterer Angaben

immer deutlich unterschieden werden.

Das VVT nach Art. 30 Abs. 1 DS-GVO sollte nicht überfrachtet werden und beispielsweise von der allgemeinen Informationssicherheit und ihren Übersichten klar getrennt bleiben.

<sup>1</sup> Siehe z.B.: <https://lfd.niedersachsen.de/download/149301>.

Da das VVT mit der Weitergabe an die Aufsichtsbehörde das Unternehmen verlässt (Art. 30 Abs. 4 DS-GVO), sollte es auch keine schutzbedürftigen, internen Informationen im Zusammenhang mit den IT-Sicherheitsmaßnahmen (z.B. Implementationsdetails technischer Sicherheitsmaßnahmen) enthalten.

### 1.3 Terminologie: VVT im engeren und im weiteren Sinne

Für das Verzeichnis nach dem Bundesdatenschutzgesetz in der bis zum 25. Mai 2018 geltenden Fassung (BDSG a.F.) hatte sich der Begriff „Verfahrensverzeichnis“ etabliert.

Greift man den veränderten Sprachgebrauch der DS-GVO auf, liegt es nahe, das Verzeichnis nach Art. 30 Abs. 1 DS-GVO als „Verarbeitungsverzeichnis“ zu bezeichnen (siehe Bitkom<sup>2</sup>). In diesem Sinne wird in der vorliegenden Praxishilfe terminologisch unterschieden zwischen:

- >> dem „Verzeichnis der Verarbeitungstätigkeiten im engeren Sinne“ (= VVT bzw. „VVT-ieS“): es enthält nur die in Art. 30 Abs. 1 DS-GVO ausdrücklich geforderten Pflichtinhalte
- >> und dem „Verzeichnis der Verarbeitungstätigkeiten im weiteren Sinne“ (= „VVT-iwS“): es umfasst das VVT-ieS sowie weitere Angaben, die zur Erfüllung der datenschutzrechtlichen Nachweispflichten erforderlich sind und bildet den Grundbestand unternehmensinterner Datenschutzdokumentation<sup>3</sup>.

Der Verantwortliche sammelt die notwendigen Angaben, die in das VVT einfließen, in einem internen Dokument, das im Folgenden als „Verarbeitungsmeldung“ bezeichnet wird.

2 Bitkom (Hrg.), Das Verarbeitungsverzeichnis, Berlin 2017, S. 7.

3 Das VVT-iwS wird in der Bitkom-Broschüre „erweitertes Verarbeitungsverzeichnis“ genannt.

### 1.4 Verpflichtete

In der Regel müssen alle Verantwortlichen (Unternehmen/Legaleinheiten/Behörden etc.) ein VVT führen.

Gem. Art. 30 Abs. 5 DS-GVO ist diese Pflicht zwar beschränkt auf Unternehmen mit einer Größe ab 250 Mitarbeitern, allerdings wird die Einschränkung durch zahlreiche Rückausnahmen wieder eingeschränkt. Die Pflicht zur Führung des VVT besteht auch bei kleineren Unternehmen, wenn alternativ

- >> die Verarbeitung mit einem besonderen Risiko verbunden ist oder
- >> sensible Daten (Art. 9 und 10 DS-GVO) verarbeitet werden oder
- >> nicht nur gelegentlich verarbeitet wird.

Allerdings lebt in diesen Fällen die Pflicht zur Dokumentation im VVT nur für die Verarbeitungen wieder auf, auf die eine der drei genannten Gegennahmen zutrifft.<sup>4</sup>

Wenn ein Verantwortlicher also „regelmäßig“ personenbezogene Daten verarbeitet, ist er unabhängig von der Mitarbeiterstärke betroffen. Die „nicht nur gelegentliche“ Verarbeitung erläutern die Aufsichtsbehörden am Beispiel der Verarbeitung von Mitarbeiterdaten. Hier sei es auch bei kleinen Unternehmen wahrscheinlich, dass sie regelmäßig Daten über ihre Mitarbeiter verarbeiten. Eine solche Verarbeitung sei dann nicht nur als „gelegentlich“ anzusehen und muss daher in das VVT aufgenommen werden.<sup>5</sup>

Zur Definition einer nur „gelegentlichen“ Verarbeitungstätigkeit bezieht sich die Artikel-29-Datenschutzgruppe auf das WP 262<sup>6</sup>. Danach darf eine Verarbeitungstätigkeit nicht regelmäßig erfolgen und muss sich außerhalb gewöhnlicher Abläufe

4 S. Artikel-29-Datenschutzgruppe, Positionspapier vom 19.04.2018, Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR, [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=624045](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045).

5 S. Positionspapier a.a.O.

6 WP 262 Guidelines on Article 49 of Regulation 2016/679 vom 06.02.2018, [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=614232](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614232), übergeleitet in EDSA, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 vom 25.05.2018, [https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation\\_de](https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_de).

zutragen, beispielsweise unter zufälligen, unvorhergesehenen Umständen und in beliebigen Zeitabständen.

Die Ausnahmeregelung läuft in der Praxis daher weitgehend ins Leere.

Nicht nur den „Verantwortlichen“ trifft die Pflicht zur Führung des VVT (Art. 30 Abs. 1 DS-GVO), sondern nach Art. 30 Abs. 2 DS-GVO hat auch der „Auftragsverarbeiter“ ein spezielles Verzeichnis (VVT für Auftragsverarbeiter – „VVT-AV“) zu führen. Dies macht im Wesentlichen die Beziehungen zwischen Kunden des Auftragsverarbeiters und seinen angebotenen Leistungen transparent. Da sich dessen Ausgestaltung fundamental vom VVT eines Verantwortlichen unterscheidet, wird auf diese spezielle Form des Verzeichnisses in dieser Praxishilfe nicht weiter eingegangen.<sup>7</sup>



Die Verantwortlichkeit für Verarbeitungen, die im Rahmen einer Auftragsverarbeitung ausgelagert werden, verbleibt beim Verantwortlichen. Der Verantwortliche hat diese Verarbeitungen in seinem VVT zu dokumentieren! Das VVT des Auftragsverarbeiters hat für ihn keinerlei Bedeutung!

Allerdings entbindet das VVT-AV einen Auftragsverarbeiter nicht von seiner Verpflichtung, als Verantwortlicher seiner eigenen Verarbeitung personenbezogener Daten ein VVT nach Art. 30 Abs. 1 DS-GVO für die eigenen Geschäftsprozesse zu führen.

### 1.5 Führung des VVT durch Vertreter in der EU

Entsprechend dem in Art. 3 Abs. 2 DS-GVO niedergelegten Marktortprinzip findet die DS-GVO selbst dann Anwendung auf die Verarbeitung personenbezogener Daten, wenn sie durch einen nicht in der Union niedergelassenen Verantwortlichen vorge-

nommen wird. Dies gilt, „wenn die Datenverarbeitung im Zusammenhang damit steht, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten ... oder das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt“.

Um des Verantwortlichen außerhalb der Union jedoch überhaupt habhaft werden zu können, trifft diesen gem. Art. 27 Abs. 1 DS-GVO die Pflicht, schriftlich einen Vertreter zu bestellen, der innerhalb der Union niedergelassen sein muss<sup>8</sup>.

Gem. Art. 27 Abs. 4 DS-GVO soll der Vertreter in der Union für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung zur Gewährleistung der Einhaltung dieser Verordnung als Anlaufstelle dienen. Aus diesem Grunde hat der Vertreter in der Union das VVT vorzuhalten. Hierbei handelt es sich um inhaltsgleiche Duplikate, sodass insoweit auf die obigen Ausführungen verwiesen werden kann.

### 1.6 Formalien

Das VVT darf in einem elektronischen Format geführt werden. Wegen der Vorlagepflicht gegenüber der Aufsichtsbehörde in Art. 30 Abs. 4 DS-GVO muss es in elektronischer oder gedruckter Form exportierbar sein. Damit ist eine einfache Zusammenstellung von internen Hyperlinks nicht tauglich, wohl aber ein Dokument, das auf beigefügte Anlagen verweist.

Aus dem Sinn des Gesetzes ergibt sich, dass das Verzeichnis dem aktuellen Stand entsprechen soll. Eine Versionierung oder die Bereithaltung einer Historie ist, auch wenn sie ggf. hilfreich sein kann, gesetzlich nicht gefordert.

Das gilt auch für die Frage, ob eine Verarbeitungsmeldung oder das Verzeichnis unterschrieben werden muss. Abgesehen davon, dass es bei der gesetzlich freigestellten elektronischen Führung schwer umzusetzen ist, gibt es auch hierfür keine gesetzlichen Anforderungen.

<sup>7</sup> S. hierzu GDD-Praxishilfe DS-GVO Vb – Verzeichnis von Verarbeitungstätigkeiten – Auftragsverarbeiter ([https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfe\\_5bVVTauftragsverarbeiter.pdf](https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfe_5bVVTauftragsverarbeiter.pdf))

<sup>8</sup> Zum Vertreter s.a. GDD-Praxishilfe DS-GVO: Der Vertreter in der Europäischen Union

### Praxis-Tipp:

Das VVT wird in einer der europäischen Sprachen geführt. Dies kann eine Konzernsprache sein, da der Verantwortliche das VVT im Wesentlichen zu eigenen Zwecken führt. Aus der DS-GVO ergibt sich keine Pflicht, das VVT in der Amtssprache der jeweiligen Aufsichtsbehörde vorzuhalten, insbesondere kann der Verantwortliche im Vorhinein nie sicher wissen, welche Behörde gerade federführend ist.<sup>9</sup>

Das VVT steht nur für interne Zwecke und auf Anfrage der zuständigen Aufsichtsbehörde zur Verfügung, es muss also nicht veröffentlicht oder für Betroffene einsehbar gemacht werden.

### 1.7 Inhalte

Das VVT ist nicht als Auflistung einzelner Verarbeitungsvorgänge, sondern als prozessorientierte Übersicht zu verstehen<sup>10</sup>.

So betont auch der EuGH in der Entscheidung „Fashion-ID“<sup>11</sup> noch einmal, dass unter „Verarbeitungen“ eine Reihe von aufeinanderfolgenden Vorgängen verstanden wird. D.h., eine Verarbeitung im Sinne der DS-GVO stellt einen Prozess dar. Mithin hat auf dieser Ebene eines Prozesses dessen Dokumentation im VVT zu erfolgen. Entscheidend ist dabei, dass über das VVT der einzelne Verarbeitungsprozess zu identifizieren ist.

Die Inhalte des VVT für Verantwortliche ergeben sich aus Art. 30 Abs. 1 DS-GVO und umfassen<sup>12</sup>:

- >> den Namen und die Kontaktdaten
  - > des Verantwortlichen;
  - > ggf. des gemeinsam mit ihm Verantwortlichen;
  - > ggf. des Vertreters in der EU;
  - > ggf. des Datenschutzbeauftragten beim Verantwortlichen;
- >> die Zwecke der Verarbeitung;
- >> die Kategorien betroffener Personen;
- >> die Kategorien personenbezogener Daten;
- >> die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden;
- >> ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation
  - > einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation;
  - > bei den in Art. 49 Abs. 1 UAbs. 2 DS-GVO genannten Datenübermittlungen die Dokumentation geeigneter Garantien;
- >> [wenn möglich,] die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- >> [wenn möglich,] eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DS-GVO.



**Vorsicht vor der Formulierung „wenn möglich“ in Art. 30 Abs. 1 lit. f und g DS-GVO: Es wird erwartet, dass diese Informationen vorliegen.**

<sup>9</sup> Das BayLDA geht davon aus, dass auf Anfrage der Behörde eine Übersetzung in der jeweiligen Amtssprache bereitzustellen sei (unveröffentlichte Stellungnahme). Diese Auffassung entbehrt jedoch einer gesetzlichen Grundlage, insbesondere ist in ErwGr 82 ausdrücklich nur von „dem“ (also einem einheitlichen) Verzeichnis die Rede.

<sup>10</sup> Das Verständnis des Verfahrensbegriffs als Bündel von Verarbeitungsschritten, wie es in Art. 18 Abs. 1 RL 95/46/EG niedergelegt war, lebt insoweit fort.

<sup>11</sup> EuGH, Urteil vom 29.07.2019 - C-40/17 - Fashion ID, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1>.

<sup>12</sup> S. im Einzelnen zur Ausgestaltung des VVT unter Kapitel „5. Anlage Muster für ein VVT“.

Die im Zusammenhang mit der Weitergabe von personenbezogenen Daten an Stellen in Drittländern geforderte Dokumentation der „Garantien“ ist in regulären Prozessen entbehrlich. Entsprechende Garantien sind ausschließlich in den Fällen des Art. 49 Abs. 1 Unterabsatz 2 DS-GVO zu dokumentieren. Die auf diese Regelung gestützten Weitergaben erfolgen nicht wiederholt. Die zu dokumentierenden Prozesse sind hingegen gerade auf Wiederholung angelegt.



**Eine Dokumentation weiterer Garantien, wie zum Beispiel eines Angemessenheitsbeschlusses der Kommission oder durch Standardvertragsklauseln kann sinnvoll sein, um den Accountability- und Transparenzpflichten ggü. Betroffenen nachkommen zu können.**

## 2. Muster von Aufsichtsbehörden

Die einheitliche Dokumentation der Verarbeitungen im VVT ist bislang (Stand 01.2020) noch nicht Gegenstand der Guidelines des Europäischen Datenschutzausschusses (EDSA). Insofern liegen noch keine einheitlichen Vorschläge bzw. Muster der Aufsichtsbehörden der EU-/EWR-Staaten vor.

Allerdings haben mittlerweile viele nationale Aufsichtsbehörden eigenständige Hinweise und Muster als Hilfestellungen für Unternehmen und Behörden ihres jeweiligen nationalen Zuständigkeitsbereichs auf ihren Webseiten veröffentlicht. Eine diesbezügliche Übersicht findet sich – ohne Anspruch auf Vollständigkeit – unter „7. Anlage Muster zum VVT von EU-Aufsichtsbehörden“. In der Regel handelt

es sich hierbei um ein Muster zu Art. 30 Abs. 1 DS-GVO, also zum VVT des Verantwortlichen.

Vergleicht man diese Muster miteinander, so stellt man eine recht große Bandbreite sowohl im Hinblick auf Detailtiefe der Dokumentation als auch bezüglich zusätzlicher – über die Anforderungen des Art. 30 Abs. 1 DS-GVO hinausgehender – Dokumentationen im VVT fest, es handelt sich also um Muster für das VVT-iwS.

Während z.B. das Muster der DSK (Deutschland) umfangreich und detailliert ausgestaltet ist, stellen viele andere Aufsichtsbehörden in der EU mit wenigen Stichworten zu füllende Tabellenblätter mit den (Mindest-)Angaben des Art. 30 Abs. 1 DS-GVO zur Verfügung, s. z.B. Frankreich, Luxemburg und Belgien.

Soweit einheitliche Vorgaben für ein VVT in einem EU-weit vertretenen Konzern gemacht werden sollen, sollten die unterschiedlichen Modelle an den jeweiligen nationalen Standorten berücksichtigt werden. Dies ist im Hinblick auf die unterschiedlichen Ausprägungen/Erwartungen der jeweiligen nationalen Aufsichtsbehörden auf der einen und der Akzeptanz in den jeweiligen nationalen Gesellschaften auf der anderen Seite, angeraten.

Allen Mustern der Aufsichtsbehörden wie auch von Verbänden<sup>13</sup> oder Softwareherstellern gemein ist es, dass es sich um unverbindliche Empfehlungen handelt. Das in Kapitel „5. Anlage Muster für ein VVT“ vorgestellte Muster beschränkt sich z.B. nur auf die „Pflichtangaben“ des Art. 30 Abs. 1 DS-GVO auf Verarbeitungs-/Prozessebene (also das VVT-ieS), während in Kapitel „6. Anlage Muster für eine Verarbeitungsmeldung“ ein Muster mit zusätzlichen Aspekten zur Dokumentation der Rechtmäßigkeit insbes. einzelner Vorgänge (Verarbeitungsschritte/ Teilprozesse) vorgestellt wird.

<sup>13</sup> S. z. B. die Muster der GMDS die speziell auf die Anforderungen des Gesundheitswesens abstellen unter [https://gesundheitsdatenschutz.org/download/Verarbeitungstaetigkeitenverzeichnis\\_Verantwortlicher.docx](https://gesundheitsdatenschutz.org/download/Verarbeitungstaetigkeitenverzeichnis_Verantwortlicher.docx)



### Praxis-Tipp:

Bei der Auswahl eines Musters sollte daher auf Kompatibilität der eigenen Zielsetzung (z.B. Erfüllung der reinen Anforderungen des Art. 30 DS-GVO oder der Dokumentation der Rechtmäßigkeit von Verarbeitungen) und der jeweiligen Intention des Muster-Erstellers geachtet werden!

## 3. Organisation des VVT

### 3.1 Prämissen

Das VVT ist die grundlegende Dokumentation unter der DS-GVO – die Datenschutz-Basis des Unternehmens bzw. der Behörde oder des Vereins. Das gilt auch und gerade mit Blick auf weitergehende Accountability-Pflichten unter der DS-GVO. Das VVT kann aber in der Praxis nur erstellt und aktuell gehalten werden, wenn:

1. Verantwortlichkeiten und Kommunikationswege festgelegt,
2. Formate definiert und
3. Prüfroutinen erstellt und durchgeführt werden.

In der Praxis hat es sich bewährt, zur Erreichung dieser Ziele eine eigene Policy VVT einzuführen (s. Beispiel in Kap. „3.3 Beispiel zur Gliederung / zum Aufbau einer Policy zum VVT“).

Alle Prozesse, die im Unternehmen eine Verarbeitung personenbezogener Daten beinhalten, müssen dezentral als Verarbeitungsmeldungen erfasst und an eine zentrale Stelle mit dem Ziel der Zusammenführung in einem Verzeichnis, dem VVT, gemeldet werden. Ebenso müssen Veränderungen kommuniziert werden, um das VVT aktuell zu halten. Insbesondere hierauf bezieht sich die Delegation der Verantwortlichkeiten und der Kommunikationswege.

Im Rahmen der Definition der Formate sind die Vorgaben für das VVT an sich zu machen, also soll

„nur“ ein VVT-ieS geführt werden oder sollen hier auch die erweiterten Angaben des VVT-iwS dokumentiert werden, um den Accountability- und Transparenzpflichten gegenüber Aufsichtsbehörden und Betroffenen nachkommen zu können.

Die Muster unter Kap. „5. Anlage Muster für ein VVT“ können z.B. für die zentrale Führung des VVT-ieS genutzt werden.

Für die Meldung/Aktualisierung der im VVT dokumentierten Verarbeitungen können Meldeformulare („Verarbeitungsmeldung“), die beispielsweise von der Fachabteilung ausgefüllt und an die führende Stelle weitergeleitet werden, ein sinnvolles Werkzeug sein (s. Kap. „6. Anlage Muster für eine Verarbeitungsmeldung“).

Prüfroutinen im Sinne eines Datenschutz-Managements stellen sicher, dass das VVT die Datenschutz-Realität im Unternehmen / in der Behörde spiegelt.

### 3.2 Rollen

Mit Blick darauf, dass die Erstellung und Führung des VVT direkt der Verantwortung des Unternehmens bzw. der Behörde obliegt, sollten die Angaben zum Verzeichnis durch das Unternehmen / die Behörde bzw. – im Wege der Delegation – durch die einzelnen Fachbereiche (als meldende, dezentrale Stellen) an eine zentrale Stelle weitergegeben werden.

Es besteht also eine Bringschuld für die notwendigen Informationen und hierzu die Etablierung einer entsprechenden Organisationsstruktur in Richtung der zentralen Führung.



Unternehmen

#### Regelungen zur

- >> Verantwortlichkeit
- >> Durchführung (Detailierung)
- >> Dokumentation
- >> Verbindung / Abgrenzung zu anderen Dokumentationspflichten
- >> Durchsetzung

Bereitstellung von Mustern / Tools / Anleitungen



Prozessverantwortlicher

#### Umsetzungsverantwortung

- >> auf der Grundlage der Organisationsanweisungen und Muster
- >> Erstellung
- >> Pflege



Zentrale Stelle

#### Führung und Prüfung

- >> Zentrale Führung des VVT
- >> Plausibilitätsprüfung
- >> Aktualität und Vollständigkeit
- >> Zur Verfügungstellung an Aufsicht bei Anforderung

**Abb.:** Rollenverteilung zur Implementierung eines VVT (nach Herweg/Müthlein, Die Überwachungsaufgabe des Datenschutzbeauftragten nach DS-GVO, 2020)

In der Datenschutz-Praxis bedeutet die gesetzliche Vorgabe des VVT zuerst einmal, das nötige Bewusstsein und die Kenntnis der gesetzlichen Anforderungen in der verantwortlichen Stelle zu schaffen. Hier kann die bereits angesprochene Policy VVT unterstützen. Danach sind die folgenden Rollen beteiligt:

**>> Meldende Stelle/n – die Bereiche, die Verarbeitungen planen und ausführen oder steuern**

In einem Unternehmen / einer Behörde werden es meist die Fachbereiche sein, die eine Verarbeitung planen und umsetzen. Hier muss der Informationsfluss zur zentralen Stelle für die Führung des VVT funktionieren. Die verantwortliche Stelle muss daher festlegen, wer wann eine Verarbeitung in welcher Form als eine Bringschuld in Richtung der zentralen, das VVT-führenden Stelle meldet. Bewährt hat sich ein Meldeformular für Erstmeldung und Aktualisierungen (Verarbeitungsmeldung, s.a. Kap. „6. Anlage Muster für eine Verarbeitungsmeldung“).

**>> Zentrale Stelle – der Bereich oder die Person, die das VVT führt und verwaltet**

Durch den Verantwortlichen wird festgelegt, wer eingehende Informationen über Verarbeitungen prüft und diese ggf. in das VVT übernimmt und dieses verwaltet. Datenschutz-Koordinator (DS-Ko) oder DSB sind hier lediglich Optionen. Dabei ist die zentrale Stelle auf den Informationsfluss durch die meldenden Stellen als deren Bringschuld angewiesen.

**>> Datenschutzbeauftragter**

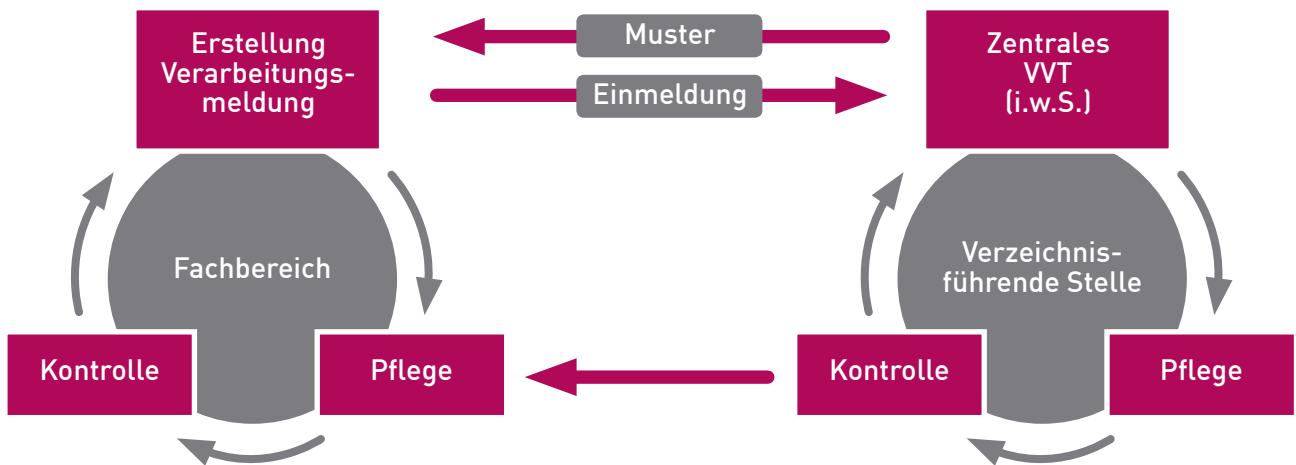
Der DSB nutzt das VVT, um seiner Überwachungsaufgabe nachkommen zu können. Er berät beim Aufbau und bei der Abgrenzung der zu dokumentierenden Prozesse. Er kann, muss aber nicht, auch die zentrale, das VVT führende Stelle sein (s.a. Kap. „4. Der DSB im Kontext des VVT“).

**>> Einsichtnehmende Stelle**

Im Fall einer Prüfung durch eine Aufsichtsbehörde hat (nur) diese das Recht, sich das VVT vorlegen zu lassen. Zu einer Regelung der Verantwortlichkeiten bei der Erstellung und Führung des VVT sollte unbedingt auch gehören, wer im Falle einer Prüfung durch eine Aufsichtsbehörde die Kommunikation mit dieser übernimmt und Einsichtnahme in oder Übergabe des VVT steuert. Dies ist keine dem DSB gesetzlich zugewiesene Rolle. Er sollte aber zumindest in die Kommunikation eingebunden werden, da die Zusammenarbeit mit der Behörde zu seinen gesetzlich festgelegten Aufgaben gehört.

**Praxis-Tipp:**

Genauso wie das Unternehmen oder die Behörde selbst entwickelt sich das VVT. Es ist daher ebenfalls best practice, dieses regelmäßig zu prüfen und anzupassen. Das kann beispielsweise im Rahmen eines IT-Ausschuss oder beim Treffen eines Datenschutz-Teams erfolgen, indem man die Prüfung des VVT regelmäßig auf die Tagesordnung setzt. Auch die zuführenden Stellen sollten regelmäßig die „gelieferten“ Verarbeitungen auf Aktualität prüfen.



Das VVT wird zentral geführt aber dezentral erstellt und gepflegt. Es ist dezentral (i.d.R. durch die Fachbereiche) sicherzustellen, dass die „Verarbeitungstätigkeiten“ personenbezogener Daten **stets aktuell gemeldet** sind.

**Abb.:** Erstellung, Pflege und Führung eines VVT (nach Herweg/Müthlein, Die Überwachungsaufgabe des Datenschutzbeauftragten nach DS-GVO, 2020)

### 3.3 Beispiel zur Gliederung / zum Aufbau einer Policy zum VVT

#### 3.3.1 Zielsetzungen der Policy

Eine Policy VVT soll:

1. Verantwortlichkeiten zur Meldung von Verarbeitungen, sowie der Erstellung und Aktualisierung des VVT festlegen und kommunizieren;
2. die Form der Dokumentation verbindlich festlegen;
3. den Informationsfluss zum Erstellen und Aktualisieren des VVTs in den Unternehmens-/Behördenprozessen verankern.

#### 3.3.2 Integration der Policy im Unternehmen

Im Unternehmen / in der Behörde existieren mutmaßlich bereits eine oder mehrere Policies oder Richtlinien zur Verankerung des Datenschutzes im Unternehmen, etwa als Datenschutz-Handbuch oder -Richtlinie. Es ist daher zu entscheiden, ob

eine Policy VVT in eine bereits bestehende Policy eingebracht oder als eigenständige Policy daneben gestellt wird.

Da es vermutlich oft die Leiter der Fachbereiche sein werden, die in neue Verarbeitungen involviert sind, könnte es ausreichen, diesen die Policy bekannt zu machen, um die Mitarbeiter nicht mit Datenschutz-Informationen und -Policies zu überfrachten.

#### Beispiel:

Policy VVT	Bekannt gemacht am	Verteiler
Enthalten in Datenschutz-Handbuch Version 1.1	17.05.2018	alle Mitarbeiter

### 3.3.3 Policy regelt: Verantwortlichkeit im Unternehmen

Verantwortlich für den Datenschutz im Unternehmen / in der Behörde und auch für das Erstellen des VVT ist als Normadressat der Verantwortliche, also das jeweilige Unternehmen oder die Behörde vertreten durch ihre Leitung. Im Rahmen der Policy ist diese Verantwortung auf operative Bereiche zu delegieren. Dabei sind zumindest folgende Verantwortlichkeiten zu bestimmen (s.a. 3.2 Rollen):

- >> Zentrale Stelle – der Bereich oder die Person, die das VVT führt und verwaltet
- >> Meldende Stelle/n – die Bereiche, die Verarbeitungen planen und ausführen oder steuern
- >> Datenschutzbeauftragter
- >> Einsichtnehmende Stelle

Die das VVT führende Stelle als zentrale Stelle ist auf den Informationsfluss der jeweils die Verarbeitungen ein- und durchführenden Fachabteilung (als meldende Stellen – Bringschuld) angewiesen. Die Policy VVT trifft hier eine klare Regelung und für den Fall eines Ausfalls oder Wechsels entsprechende Zugriffsberechtigungen für weitere Ansprechpartner im Unternehmen.

In der Praxis wird die VVT führende Stelle als zentrale Stelle oft vom DS-Ko oder DSB geführt, auch wenn dies nur zwei Optionen sind. Es wird folgender Vorteil gesehen: diese haben die Fachkunde zu entscheiden, ob eine Verarbeitung in das VVT übernommen wird oder vielleicht doch eher Teil eines bereits beschriebenen Prozesses ist.

#### Beispiel:

VVT wird geführt von / Meldung an	Zugriffsberechtigungen VVT
Datenschutzkoordinator	Datenschutzbeauftragter Geschäftsführer

### 3.3.4 Policy legt fest: Vorlage zum Erstellen eines VVT

Es gibt unterschiedliche Vorlagen für das VVT, z.B. unter „5. Anlage Muster für ein VVT“. Sinnvoll erscheint, sich für eine Vorlage als festes Format zu entscheiden und diese dann konsequent und einheitlich für alle identifizierten Verarbeitungen im Unternehmen anzuwenden.

#### Beispiel:

Vorlage zur Beschreibung der Verarbeitung	Speicherort
Vorlagevvt_gdd2019.	Datenschutz:\vvt docx

Sprache/n	Export möglich als
Deutsch	>> Ausdruck >> pdf

### 3.3.5 Policy legt fest: Meldung einer Verarbeitung erfolgt durch/mittels

Alle Verarbeitungen, die personenbezogene Daten beinhalten, sind der zentralen Stelle zu melden. In der Praxis hat sich dafür ein einheitliches Meldeformular bewährt (s. z.B. „6. Anlage Muster für eine Verarbeitungsmeldung“, das neben den Pflichtangaben zum VVT auch weitere Angaben zur Rechenschaftspflicht enthält). Neben der Dokumentation und Pflege bestehender Verarbeitungen sind insbesondere Änderungen oder Neueinführungen sowie die Einstellung von Verfahren Auslöser für Meldungen.

**Beispiel:**

<b>Verantwortlich für Meldung / Verarbeitung an VVT führende Stelle</b>	<b>Vorlage Meldeformular Verarbeitung</b>
<i>Leiter Fachbereich</i>	<i>Datenschutz:\vvt\MeldeformularVerarbeitung_bearbeitet_20190515.docx</i>

**3.3.6 Policy regelt: regelmäßige Kontrolle der Verarbeitungen und des VVT**

Im Rahmen eines aktiven und von der DS-GVO geforderten kontinuierlichen Verbesserungsprozesses im Rahmen eines Datenschutz-Managements sind die mit dem VVT dokumentierten Verarbeitungen regelmäßig zu überprüfen, zumindest hinsichtlich:

- >> Sind die dokumentierten Verarbeitungen noch aktuell?
- >> Haben sich in den dokumentierten Verarbeitungen Änderungen ergeben und sind diese gemeldet worden?
- >> Sind neue Verarbeitungen hinzugekommen und gemeldet worden?
- >> Sind die beschriebenen Verantwortlichkeiten noch aktuell?

**Praxis-Tipp:**

Ist im Unternehmen beispielsweise ein Datenschutz-Team aktiv, das sich regelmäßig trifft, sollte hier auch eine Überprüfung der dokumentierten VVTs erfolgen. Weiterhin sollten die Leiter der Fachbereiche zu regelmäßigen Meldungen bzw. Überprüfungen verpflichtet werden.

**Beispiel:**

<b>Verarbeitung zuletzt kontrolliert am</b>	<b>Meldung erfolgt an</b>
<i>31.10.2019</i>	<i>Datenschutzbeauftragte/n</i>

<b>Meldung erfolgt durch</b>	<b>Meldung erfolgt mittels</b>
<i>Leiter IT</i>	<i>MeldeformularVerarbeitung_bearbeitet_20190515.docx</i>

**3.3.7 Policy legt fest: wer kommuniziert mit der Aufsichtsbehörde**

Nur eine Datenschutz-Aufsichtsbehörde hat ein Recht auf Einsichtnahme in das VVT. Anlaufstelle für die Aufsichtsbehörde ist neben der Unternehmens-/Behördenleitung der ihr gemeldete DSB - sofern im Unternehmen vorhanden. Da „Anlaufstelle“ nicht die operative Bearbeitung beinhaltet, legt die Policy fest, wer im Fall einer Anfrage durch eine Aufsichtsbehörde die Kommunikation übernimmt und entscheidet, in welcher Form und eventuell auch wie umfangreich das VVT zur Verfügung gestellt wird. Letzteres ist besonders dann von Relevanz, wenn das VVT mit weiterführenden Informationen verknüpft ist (VVT-iwS). Die Aufsichtsbehörde wird im ersten Anlauf lediglich den Anspruch auf die Pflichtangaben des Artikel 30 DS-GVO (VVT-ieS) haben. Es ist auch im Sinne einer effizienten Kommunikation naheliegend, nur diese Informationen zur Verfügung zu stellen.

## Beispiel:

Verantwortlich für Kommunikation mit Aufsichtsbehörde	Cc Kommunikation
1. Datenschutzbeauftragter	>> Datenschutzkoordinator
2. Datenschutzkoordinator	>> Geschäftsführer >> (...)
3. Geschäftsführer	



Da das VVT-ieS bei einer Prüfung durch die Aufsichtsbehörde das Unternehmen/die Behörde auch verlassen kann, sollte es keine schutzbedürftigen, internen Informationen, beispielsweise im Zusammenhang mit den IT-Sicherheitsmaßnahmen (z.B. Implementationsdetails technischer Sicherheitsmaßnahmen) enthalten. Bei einer Erweiterung zum VVT-iwS sollte eine klare Trennung für die Einsichtnahme der Aufsichtsbehörde einfach möglich sein.

## 3.3.8 Checkliste Policy VVT

Check Policy	Geregelt?
Verantwortlichkeit: wer führt das VVT?	<input checked="" type="checkbox"/>
Verantwortlichkeit: wer hat Zugriff auf das VVT?	<input checked="" type="checkbox"/>
Verantwortlichkeit: wer meldet Verarbeitungen an wen?	<input checked="" type="checkbox"/>
Verantwortlichkeit: wer kontrolliert wann die Aktualität des VVT?	<input checked="" type="checkbox"/>
Anlagen Vorlage VVT und Meldeformular enthalten?	<input checked="" type="checkbox"/>
Policy veröffentlicht/kommuniziert?	<input checked="" type="checkbox"/>

## 4. Der DSB im Kontext des VVT

Der DSB hat gemäß der ihm durch die DS-GVO übertragenen Aufgaben die Funktion, den Verantwortlichen bzw. die Beschäftigten, die mit einer Verarbeitung personenbezogener Daten betraut sind, zu beraten und die Einhaltung der Datenschutzvorschriften zu überwachen. Insofern fällt dem DSB eine unterstützende Aufgabe zu, die grundsätzlich frei von operativen Tätigkeiten ist.

Das VVT ist unmittelbar vom Verantwortlichen zu führen und ergibt sich nicht aus den Aufgaben des DSB; diese Aufgabe (aber nicht die Verantwortung selbst) kann aber delegiert werden und wird in der Datenschutz-Praxis oft an den Datenschutz-Koordinator oder DSB übertragen. Auch der Europäische Datenschutz-Ausschuss (EDSA) erklärt es für zulässig, den DSB mit der Erstellung, Führung und Pflege zu betrauen.<sup>14</sup>

<sup>14</sup> Der EDSA ist nach der DS-GVO die „Nachfolge-Organisation“ der Artikel-29-Datenschutzgruppe. S. hier: WP 243 Guidelines on Data Protection Officers (rev. 1) vom 05.04.2017, [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44100](http://ec.europa.eu/newsroom/document.cfm?doc_id=44100) – Diese Leitlinie gehört zu den vom EDSA gebilligten Leitlinien, s. <https://edpb.europa.eu/node/89>.

Im Hinblick darauf, dass der DSB in der Ausübung seiner Aufgaben frei von Interessenskonflikten sein muss, können hiermit nur administrative Funktionen gemeint sein. Daher kann die Verantwortung für das VVT nicht auf den DSB übertragen werden. Die Erstellung und Pflege der Verarbeitungsmeldungen bleibt also eine Bringschuld des Verantwortlichen, in der Regel seiner Fachbereiche.

Zuvorderst wird es im Rahmen seiner Beratungsfunktion die Aufgabe des DSB sein, für die Umsetzung des VVT in der Organisation und in den Prozessen zu sorgen. So ist für das VVT eine einheitliche Struktur sowie ein zentraler Anlageort sicherzustellen. Des Weiteren sind eine Policy zum VVT und die erforderlichen Angaben für eine Verarbeitungsmeldung auszugestalten und in der Organisation zu implementieren (s. Kap. „3. Organisation des VVT“).

Im Rahmen der Policy zum VVT sind die Fachbereiche zu verpflichten, Verarbeitungsmeldungen für neue oder geänderte Verarbeitungen zu erstellen und an die das VVT führende Stelle weiterzuleiten. Dabei können die Fachbereiche im Zweifelsfall auf die beratende Tätigkeit des DSB zurückgreifen.

Zweckmäßigerweise sollten diese Verarbeitungsmeldungen durch den DSB bzw. einem eventuell vorhandenem Datenschutzteam zusammengeführt werden. So kann die Verarbeitungsmeldung direkt auf Rechtmäßigkeit und Vollständigkeit geprüft werden, was der Überwachungsaufgabe des DSB zugutekommt.

Unabhängig von Verarbeitungsmeldungen der Fachbereiche kann es für den DSB zweckmäßig sein, regelmäßig eine Überprüfung des VVT auf Vollständigkeit und Aktualität anzustoßen, da Prozessänderungen in den Fachbereichen häufig gar nicht oder aber verspätet zu Verarbeitungsmeldungen führen.

### Die Aufgaben des DSB im Überblick:

- >> Beratungsthemen des DSB:
  - > Erstellung und Aktualisierung einer VVT Struktur
  - > Festlegung eines zentralen Ablageortes
  - > Erstellung und Aktualisierung einer Policy zum VVT

- > Erstellung und Aktualisierung des Musters einer Verarbeitungsmeldung
- > Implementierung der Policy zum VVT und des Musters einer Verarbeitungsmeldung in der Organisation
- > Beratung der Fachbereiche zur Verarbeitungsmeldung
- > Prüfung der Verarbeitungsmeldung auf Vollständigkeit und Rechtmäßigkeit der Verarbeitung
- > Zusammenführung der Verarbeitungsmeldungen
- > Anstoß zur regelmäßigen Aktualisierung des VVT

### >> Überwachung durch den DSB

- > Der Überwachungsauftrag des DSB hinsichtlich des VVT ist auf die Feststellung gerichtet, ob die
  - Erstellung, Pflege und Kontrolle der Verfahrensmeldung auf der Ebene der Fachprozesse durch die Fachbereiche
  - Zentrale Führung des VVT und
  - Aktualität und Vollständigkeit des VVT

angemessen und wirksam geregelt und die Umsetzung sichergestellt sind.

## 5. Anlage Muster für ein VVT

Das VVT stellt die Zusammenführung der einzelnen gemeldeten Verarbeitungstätigkeiten dar (s.o. „3. Organisation des VVT“). Die Anforderungen an die Inhalte des VVT ergeben sich aus Art. 30 Abs. 1 DS-GVO, siehe hierzu auch oben „1.7 Inhalte“.

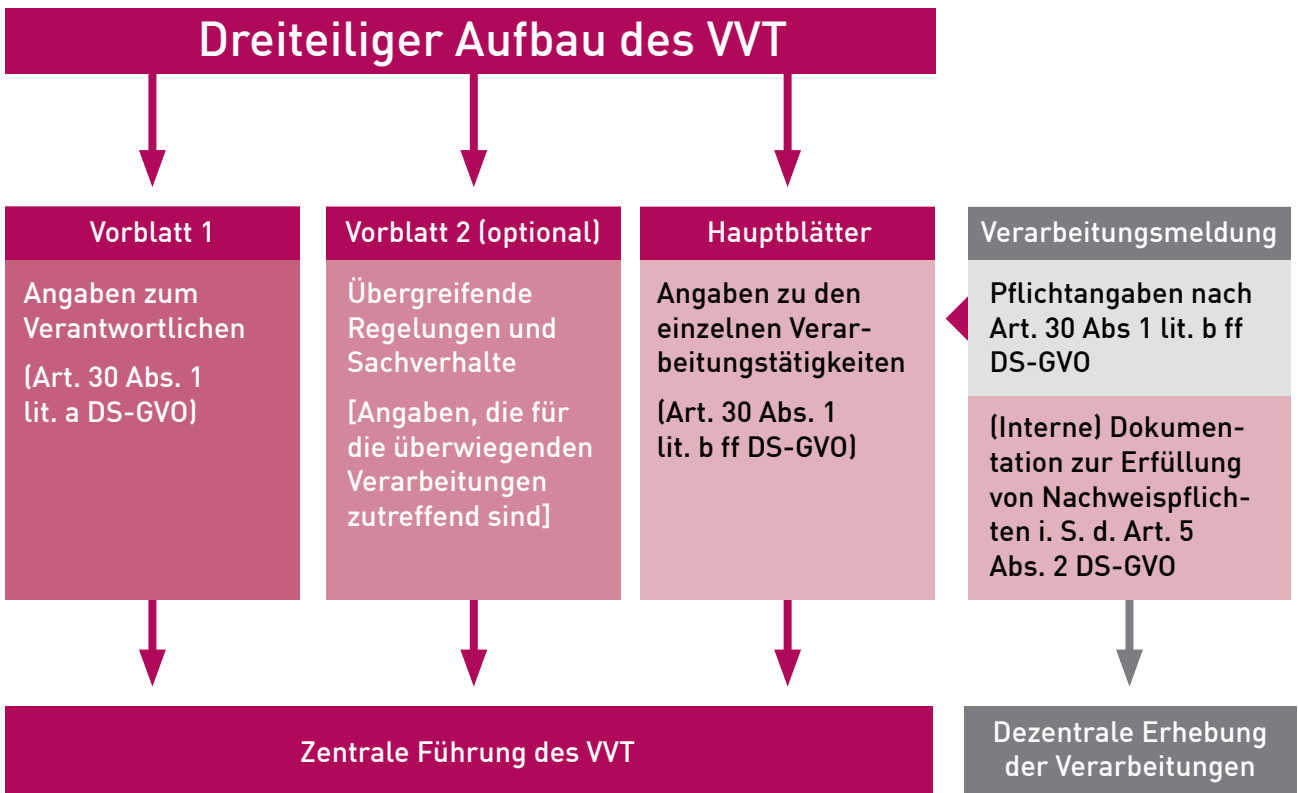
Im **Vorblatt 1** werden Angaben zum Verantwortlichen erfasst, im **Vorblatt 2** Angaben zu übergreifenden Regelungen und Sachverhalten („5.1 Muster Vorblatt für ein VVT“). Hierdurch sollen sich ansonsten wiederholende Angaben nur einmal dokumentiert werden, um den Pflegeaufwand zu erleichtern.

Hieran schließt sich die Dokumentation der einzelnen Verarbeitungstätigkeiten an (s. „5.2 Muster Hauptblatt für ein VVT für Angaben zu den einzelnen Verarbeitungstätigkeiten“)(„**Hauptblätter**“). Dieses



Muster kann auch zur dezentralen Erhebung genutzt werden.

Soweit zur unternehmensinternen Dokumentation weitergehende Angaben, die zur Erfüllung der Nachweispflichten i.S.d. Art. 5 Abs. 2 DS-GVO (für das VVT-iwS) beitragen, direkt miterhoben werden sollen, wird in Kap. „6. Anlage Muster für eine Verarbeitungsmeldung“ ein separates Muster bereitgestellt. Es gliedert sich in die Pflichtangaben des VVT (Nr. 1-9 – können direkt in das VVT übernommen werden) und weitergehende Angaben zur Erfüllung der Rechenschaftspflichten i.S.d. Art. 5 Abs. 2 DS-GVO (Nr. 10-27 – dient der internen Dokumentation).



**Abb.:** Aufbau VVT-ieS und Speisung aus Verarbeitungsmeldungen

## 5.1 Muster Vorblatt für ein VVT

# Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen<sup>15</sup>

## Vorblatt 1

### Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DS-GVO)

#### 1. Verantwortlicher (= Unternehmen/Legaleinheit)

*[Name, ladungsfähige Anschrift]*

#### 2. Gesetzlicher Vertreter (= Geschäftsführung)

*[Name/Kontaktdaten]*

#### 3. Vertreter in der EU (gemäß Art. 27 DS-GVO)

*[Name/ladungsfähige Anschrift]*

#### 4. Datenschutzbeauftragter

*[Name/Kontaktdaten]*

## Vorblatt 2 (optional)

### Übergreifende Regelungen und Sachverhalte

#### 5. Regelungen zur Datensicherheit

*[Verweis auf übergreifende IT-Sicherheitskonzepte, die grds. für alle Verarbeitungstätigkeiten gelten.]*

#### 6. Regelungen zur Datenlöschung

*[Verweis auf übergreifende Löschkonzepte, die grds. für alle Verarbeitungstätigkeiten gelten.]*

#### 7. Sachverhalte zu Drittlandsübermittlungen

*[Verweis auf übergreifende Drittlandsübermittlungen, die grds. alle oder mehrere Verarbeitungstätigkeiten betreffen.]*

<sup>15</sup> Das Muster ist für den Einsatz in Unternehmen ausgerichtet. Für den Einsatz in Behörden/öffentlichen Stellen sind die Begrifflichkeiten der freien Wirtschaft gegen solche in der jeweiligen Behörde/öffentlichen Stelle üblichen zu ersetzen.

### 1. Verantwortlicher

Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DS-GVO).

Angaben: Name/Firma, ladungsfähige Anschrift

### 2. Gesetzlicher Vertreter

Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter

Angaben: Namen der geschäftsführenden Personen

Ggf. kann hier einfach ein Link auf das Web-Im-pressum eingetragen werden.

### 3. Vertreter in der EU

Bei Unternehmen ohne Niederlassung in der Europäischen Union ist hier der benannte Vertreter des Verantwortlichen (Art. 4 Nr. 17 DS-GVO, Art. 27 Abs. 1 DS-GVO) anzugeben.

### 4. Datenschutzbeauftragter

Vom Verantwortlichen bestellter Datenschutzbeauftragter [Name, Kontaktdaten]

### 5. Regelungen zur Datensicherheit

Gegebenenfalls Verweise auf übergreifende Regelungen (falls solche existieren, die grds. alle Verarbeitungen betreffen) – Der Verweis an dieser Stelle auf übergreifende Regelungen entbindet nicht von der Dokumentation von ggf. erforderlichen Abweichungen zu den einzelnen Verarbeitungstätigkeiten.

Verweis z.B. auf ein IT-Sicherheitskonzept, das alle Verarbeitungstätigkeiten einschließt. Eventuell auch Verweise auf relevante Dokumente eines Informations-Sicherheits-Management-Systems (ISMS) nach ISO 27001.

### 6. Regelungen zur Datenlöschung

Verweis auf Löschkonzepte, die grds. für alle Verarbeitungen gelten.

### 7. Sachverhalte zu Drittlandsübermittlungen

Ein Verweis auf Drittlandsübermittlungen ist hier sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen betroffen sind.

5.2 Muster Hauptblatt für ein VVT für Angaben zu den einzelnen Verarbeitungstätigkeiten

## Verzeichnis von Verarbeitungstätigkeiten

Hauptblatt Nr.

### Angaben zur Verarbeitungstätigkeit und zur Verantwortlichkeit (Art. 30 Abs. 1 lit. b ff. DS-GVO)

1. Bezeichnung der Verarbeitungstätigkeit

2. Verantwortlicher Fachbereich/sonstige Zuordnungskennzeichen (optionaler Inhalt)

3. Bei gemeinsamer Verantwortlichkeit:

*Name und Kontaktdaten (ladungsfähige Anschrift) des/der weiteren Verantwortlichen*

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

5. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)

Betroffene Personengruppen

Kategorien personenbezogener Daten

6. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden (Art. 30 Abs. 1 lit. d DS-GVO)

*[interne, externe – auch im Konzern, eingebundene Dienstleister]*

**Fortsetzung Muster Hauptblatt für ein VVT für  
Angaben zu den einzelnen Verarbeitungstätig-  
keiten**

**7. Datenübermittlungen in Drittländer oder internationale Organisationen  
(Art. 30 Abs. 1 lit. e DS-GVO)**

>> Übermittlung  Ja  Nein

>> Name des Drittlandes/der internationalen Organisation (DS-GVO):

>> Falls zutreffend, Angaben zu geeigneten Garantien bei Datenübermittlungen auf der Grundlage von Art. 49 Abs. 1 UAbs. 2 DS-GVO:

**8. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien  
(Art. 30 Abs. 1 lit. f DS-GVO)**

**9. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen  
(TOM; Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)**

*[Bezug zum IT-Sicherheitskonzept, Abweichungen bzw. Ergänzungen  
oder (soweit zutreffend): Link auf TOM (des Auftragsverarbeiters) hier anführen  
oder (soweit zutreffend): Verweis auf Datenschutz-Zertifizierung etc.]*

## 1. Bezeichnung der Verarbeitungstätigkeit

Eindeutige Bezeichnung der dokumentierten Verarbeitung/der Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen geläufige Bezeichnung des Fachprozesses gewählt werden.

Empfehlung: Der **Name der Verarbeitung sollte unabhängig von einzelnen IT-Tools sein**, die ggfs. im Rahmen der Verarbeitung / des Prozesses zum Einsatz kommen.

Beispiele:

- >> Allgemeine Kundenverwaltung
- >> Customer-Relationship-Management (CRM)

## 2. Verantwortlicher Fachbereich/sonstige Zuordnungskennzeichen

Dies ist bezogen auf die Pflichtangaben des Art. 30 Abs. 1 DS-GVO eine optionale Angabe, um unternehmensintern die Zuordnung der dokumentierten Verarbeitungstätigkeit im VVT zu einem bestimmten Fachbereich und dessen erweiterter Dokumentation herstellen zu können.

Dies kann z.B. mittels der Funktionsbezeichnung des Fachbereiches, oder eines sonstigen Zuordnungskennzeichens (z.B. eine eindeutige Identifikationsnummer) erfolgen.

## 3. Bei gemeinsamer Verantwortlichkeit

Falls mehrere Verantwortliche gemeinsam für die Verarbeitungstätigkeiten verantwortlich sind, bspw. innerhalb einer Unternehmensgruppe, sind hier Name und Kontaktdaten (ladungsfähige Anschrift) des oder der weiteren Verantwortlichen anzugeben (Firma/ladungsfähige Anschrift; Art. 30 Abs. 1 lit. a DS-GVO, Art. 26 Abs. 1 DS-GVO).

## 4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

Beispiele:

- >> Verarbeitungstätigkeit: „Allgemeine Kundenverwaltung“; verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso“
- >> Verarbeitungstätigkeit: „Customer-Relationship-Management“; verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Kundenbeziehungen, Marketing, Neukundenakquise, Kundenbindungsmaßnahmen, Kundenberatung, Beschwerdemanagement, Kündigungsprozess“

Eine Verarbeitungstätigkeit kann mehrere Teil-Geschäftsprozesse (der EuGH spricht von „Vorgängen“) zusammenfassen. Dementsprechend kann eine Verarbeitung auch mehrere Zwecke umfassen, so dass auch mehrere Zweckbestimmungen angegeben werden können.

Die Detailtiefe hängt von der Geschäftstätigkeit des Unternehmens ab.

Es können neben dem Fachprozess auch begleitende mitarbeiterbezogene Unterstützungsprozesse vorliegen, wie z.B. zur Personalführung/-einsatzplanung. Diese können entweder als Teil einer anderen Verarbeitung oder als eigene Verarbeitung beschrieben sein.

## 5. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)

Als betroffene Personengruppen kommen beispielsweise Kunden, Interessenten, Arbeitnehmer, Schuldner, Versicherungsnehmer usw. in Betracht.

Den einzelnen Personengruppen sind die jeweils auf sie bezogenen verwendeten Daten oder Datenkategorien zuzuordnen. Damit sind keine personenbezogenen Daten, sondern „Datenbezeichnungen“/

Datenkategorien gemeint (z.B. „Adresse“, „Geburtsdatum“, „Bankverbindung“). Werden solche Datenkategorien angegeben, so müssen diese so konkret wie möglich sein. Nicht ausreichend, da zu allgemein, sind etwa Angaben wie „Kundendaten“ oder Ähnliches.

Beispiele:

- >> Kunden: Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax- und E-Mail-Daten), Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließl. Kundenentwicklung, Produkt- bzw. Vertragsinteresse, Statistikdaten, Abrechnungs- und Leistungsdaten, Bankverbindung
- >> Beschäftigtendaten (Lohn und Gehalt): Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, etc.

### 6. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden (Art. 30 Abs. 1 lit. d DS-GVO)

Empfängerkategorien sind insbesondere am Prozess beteiligte weitere Stellen des Unternehmens/

Konzerns oder andere Gruppen von Personen oder Stellen, die Daten – ggf. über Schnittstellen – erhalten, z.B. in den Prozess eingebundene weitere Fachabteilungen, Vertragspartner, Kunden, Behörden, Versicherungen, Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.

Laut Gesetz sind nur die Kategorien von Empfängern anzugeben. Bei genauerer Darstellung sind spätere Änderungen zu berücksichtigen und die regelmäßige Pflege der Angaben ist zu gewährleisten.

### 7. Datenübermittlungen in Drittländer oder internationale Organisationen (Art. 30 Abs. 1 lit. e DS-GVO)

Drittländer sind solche außerhalb der EU/des EWR. Beispiele für internationale Organisationen: Institutionen der UNO, der EU.

Lediglich in Ausnahmefällen wird es erforderlich sein, Angaben zu geeigneten Garantien anzugeben, nämlich dann, wenn keine der genannten Garantien vorliegt, sind hier andere getroffene Garantien zu dokumentieren (Art. 49 Abs. 1. UAbs. 2 DS-GVO)<sup>16</sup>.

**16** Dies betrifft nur folgenden Ausnahmefall:

Die Übermittlung kann nicht auf

> eine Bestimmung der Art. 45 oder 46 – einschließlich der verbindlichen internen Datenschutzvorschriften oder

> eine der Ausnahmen für einen bestimmten Fall gemäß Art. 49 Abs. 1 Satz 1 Buchstaben a bis g

gestützt werden und folgende Bedingungen sind alle erfüllt:

> die Übermittlung erfolgt nicht wiederholt,

> betrifft nur eine begrenzte Zahl von betroffenen Personen,

> ist für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen,

> der Verantwortliche hat alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung angemessene Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen,

> der Verantwortliche hat die Aufsichtsbehörde von der Übermittlung in Kenntnis gesetzt und

> der Verantwortliche hat die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen unterrichtet.

D.h. falls es sich bspw. um ein Drittland mit Angemessenheitsbeschluss der EU-Kommission handelt, EU-Standarddatenschutzklauseln abgeschlossen wurden oder verbindliche interne Datenschutzvorträge vorliegen, sind nähere Angaben zu den Garantien **nicht** erforderlich.

### 8. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 lit. f DS-GVO)

Anzugeben sind hier die konkreten Aufbewahrungs-/Löschfristen, die in Verarbeitungstätigkeiten implementiert sind, bezogen auf einzelne Verarbeitungsschritte, falls unterschiedlich.

Soweit diese in einem Löschkonzept dokumentiert sind, reicht der konkrete Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.

### 9. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

>> Soweit für die Verarbeitung die Vorgaben des übergreifenden Sicherheitskonzepts (**siehe Vorblatt 2 Nr. 5**) Anwendung finden, kann hierauf verwiesen werden. Eventuelle Abweichungen sind zusätzlich zum Verweis zu dokumentieren.

- >> Soweit sich die technischen und organisatorischen Maßnahmen aus anderen vorhandenen Sicherheitsrichtlinien/Konzepten/Zertifizierungen, z.B. aus dem Sicherheitskonzept eines eingebundenen Auftragsverarbeiters, ergeben, ist ein konkreter Verweis hierauf ausreichend. Eventuelle Abweichungen sind zusätzlich zum Verweis zu dokumentieren.
- >> Soweit für die technischen und organisatorischen Maßnahmen keine der vorgenannten Dokumentationen vorliegen, sind sie hier im Einzelnen zu dokumentieren.
- >> Ein Verweis auf das Vorhandensein einer Datenschutz-Folgenabschätzung ist eine sinnvolle **optionale** Angabe, um darüber aufzuzeigen, dass eine individuelle Betrachtung der Risiken erfolgt ist und angemessene Sicherheitsvorkehrungen ergriffen und dokumentiert wurden.



## 6. Anlage Muster für eine Verarbeitungsmeldung

Die Verarbeitungsmeldung dient den Unternehmen dazu, die Verarbeitungen personenbezogener Daten mit den erforderlichen Angaben zur Erfüllung der Nachweispflichten i.S.d. Art. 5, 24 DS-GVO zu dokumentieren (s.a. 5. Anlage Muster für ein VVT). Darüber hinaus stellt sie ein wichtiges Werkzeug für

die Beratung der Fachbereiche des Unternehmens im Hinblick auf ihre Datenschutzpflichten dar. In der Praxis hat es sich bewährt, dass die Fachbereiche die Verarbeitungsmeldung – unter Nutzung der Erläuterungstexte – zunächst, soweit wie ihnen möglich ist, selbst ausfüllen und im zweiten Schritt eine Vervollständigung mit Unterstützung der Datenschutzorganisation erfolgt.

### Verarbeitungsmeldung

#### Angaben für das Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 DS-GVO

0. Verantwortliches Unternehmen<sup>17</sup>:

1. Bezeichnung der Verarbeitungstätigkeit:

2. Verantwortlicher Fachbereich/sonstige Zuordnungskennzeichen:

3. Bei gemeinsamer Verantwortlichkeit:

*Name und Kontaktdaten (ladungsfähige Anschrift) des/der weiteren Verantwortlichen*

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit:

5. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)

Betroffene Personengruppen

Kategorien personenbezogener Daten

6. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden (Art. 30 Abs. 1 lit. d DS-GVO)

*[interne, externe – auch im Konzern, eingebundene Dienstleister]*

<sup>17</sup> Nur erforderlich, soweit das Muster in einem Konzern/einer Unternehmensgruppe verwendet wird und die Meldungen zentral im Konzern/der Gruppe zusammengeführt werden.

**7. Datenübermittlungen in Drittländer oder internationale Organisationen**  
(Art. 30 Abs. 1 lit. e DS-GVO)

>> Übermittlung  Ja  Nein

>> Name des Drittlandes/der internationalen Organisation (DS-GVO):

>> Falls zutreffend, Angaben zu geeigneten Garantien bei Datenübermittlungen auf der Grundlage von Art. 49 Abs. 1 UAbs. 2 DS-GVO:

**8. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien**  
(Art. 30 Abs. 1 lit. f DS-GVO)

Gemäß folgender Beschreibung (ggfs. unter Verweis auf ein Löschkonzept):

**9. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen**  
(TOM; Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

[ggfs. hier die Maßnahmenbeschreibungen einfügen oder verlinken]

Bezug zum IT-Sicherheitskonzept, Abweichungen bzw. Ergänzungen:

Gemäß folgender Zertifizierung:

Gemäß Vereinbarung mit dem Dienstleister:

Gemäß folgender Beschreibung:

**Weitergehende Angaben zur Verarbeitung zur Erfüllung  
der Rechenschaftspflichten gem. Art. 5 (2) DS-GVO**

**10. Datum und Art der Meldung**

Datum

Neuanmeldung

Löschung

Änderung

**11. (Geplanter) Beginn der Verarbeitung**

Datum

**12. Wesentliche Prozessschritte**

**13. Ergänzende Dokumente und Unterlagen**

(ggfs. Anlagen hier einbinden oder verlinken)

14. Verarbeitung von besonderen Kategorien personenbezogener Daten

- Es werden besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO) oder Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO) verarbeitet.

15. Rechtsgrundlage der Verarbeitungstätigkeit

- Vertrag oder Vertragsanbahnung mit dem Betroffenen (Art. 6 Abs. 1 b) DS-GVO.tet.
- Berechtigtes Interesse des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 f) DS-GVO):
- Spezialgesetzliche Regelung außerhalb der DS-GVO:
- Einwilligung des Betroffenen (Art. 6 Abs. 1 a) DS-GVO:
- Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses (§ 26 BDSG-neu)
- Kollektivvereinbarung (z.B. Betriebsvereinbarung, Tarifvertrag):
- Sonstiges:

16. Weitere Angaben bei gemeinsamer Verantwortlichkeit gem. Art. 26 DS-GVO

Auf welche Vorgänge bezieht sich die gemeinsame Verantwortlichkeit:

Liegt eine Vereinbarung der gemeinsam Verantwortlichen vor:

Liegen die diesbezüglichen wesentlichen Informationen der Betroffenen vor:

Erfüllung der Informationspflichten:

17. Empfänger, denen die Daten offengelegt worden sind oder noch offengelegt werden

	Empfänger	Empfänger-Kategorie	EU/EWR/Drittland
an Empfänger <b>innerhalb</b> des Verantwortlichen			<input type="checkbox"/> EU/EWR <input type="checkbox"/> Drittland: <input type="text"/>
an Empfänger (Dritte) <b>außerhalb</b> des Verantwortlichen			<input type="checkbox"/> EU/EWR <input type="checkbox"/> Drittland: <input type="text"/>

## 18. Eingebundene Dienstleister

Dienstleister	Auftrags- verarbeitung	Ort der Datenverarbeitung	Ggfs. vertragliche Vereinbarungen
	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	<input type="checkbox"/> EU/EWR <input type="text"/> <input type="checkbox"/> Drittland <input type="text"/>	
	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	<input type="checkbox"/> EU/EWR <input type="text"/> <input type="checkbox"/> Drittland <input type="text"/>	

## 19. Garantien im Falle von Datenübermittlungen in Drittländer oder internationale Organisationen (vgl. Pkt. 17 und 18)

- Anerkannter Drittstaat
- Standarddatenschutzklauseln für den Drittlandstransfer
- Aufsichtsbehördlich genehmigter Vertrag
- BCR gem. Art. 47 DS-GVO
- Andere getroffene Garantien (Art. 49 Abs. 1. UAbs. 2 DS-GVO):

## 20. Beteiligte IT-Systeme

- DV-Anlagen:
- Software (und ggf. Unterprogramme):
- Schnittstellen:
- Sonstige Programme, Anwendungen und IT:

Alternativ ist auch der Verweis auf externe Dokumentation möglich:

(ggfs. Link hier einfügen)

Ggfs. Angaben zur Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten in Nicht-Produktivsystemen:

## 21. Informationspflichten

Datenschutzinformation mittels (z.B. Information am (Arbeits-) Vertrag, am Formular, an der Einwilligung):

Bitte ggfs. Datenschutzinformation hier einfügen:

Datenschutzerklärung der Webseite – bitte Link oder Ausdruck hier einfügen:

Sonstiges:

Zu welchem Zeitpunkt erfolgt die Information?

## 22. Durchführung der Verarbeitung für weitere Unternehmen als Dienstleistung

Wird die Verarbeitung auch dienstleistend für weitere Unternehmen, z.B. als Shared Service im Konzern/in der Gruppe durchgeführt?

Ja, auf Grundlage folgender vertraglicher Vereinbarungen:

Nein

## 23. Zugriffsberechtigungen

Wie sind die Zugriffsberechtigungen geregelt?

Bitte beschreiben Sie die Personengruppen und Berechtigungsrollen mit Umfang und Art des Datenzugriffs, sowie den Prozess zur Erlangung und Verwaltung der Berechtigungen (alternativ Verweis auf ein eingebettetes oder verlinktes Berechtigungskonzept):

## 24. Umfang der Verarbeitung

Angaben zum Umfang der Verarbeitung:

Ungefähre Anzahl der Betroffenen/Datensätze, sowie Anzahl Datenfelder pro Betroffenen/Datensatz:

## 25. Risiko der Verarbeitung und Datenschutz-Folgenabschätzung

>> Wurde eine Bewertung der Datenschutz-Risiken durchgeführt (unter Berücksichtigung der Blacklists der Datenschutz-Aufsichtsbehörden – „Schwellenwert-Analyse“)?

Ja, mit folgendem Ergebnis:

Nein

>> Falls im Rahmen der „Schwellenwert-Analyse“ ein „Hohes Risiko“ ermittelt wurde, bitte die erforderliche Dokumentation der Risiken und der ergriffenen Schutzmaßnahmen in Form einer Datenschutz-Folgenabschätzung hier einbetten:

## 26. Wahrung der (weiteren) Betroffenenrechte

Die weiteren Betroffenenrechte (Recht auf Auskunft, Berichtigung, Einschränkung, Widerspruch, Datenübertragbarkeit sowie im Zusammenhang mit automatisierten Entscheidungen im Einzelfall einschließlich Profiling) werden wie folgt sichergestellt:

## 27. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Wie wird der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sichergestellt?

Hier bitte Beschreibungen oder ausgefüllte Checklisten einbetten:

## Erläuterungen

### Angaben für das Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 DS-GVO

#### 0. Verantwortliches Unternehmen

Benennung des für die Datenverarbeitung verantwortlichen Unternehmens.

Diese Angabe in der Verarbeitungsmeldung ist vornehmlich im Konzern bzw. in Unternehmensgruppen relevant, um sicherzustellen, dass die Verarbeitungsmeldungen der unterschiedlichen Unternehmen dem richtigen Verzeichnis zugeordnet werden müssen.

Die Angabe kann bei Einzelunternehmen, bei denen die Zuordnung der Verantwortlichkeit eindeutig ist, entfallen.

#### 1. Bezeichnung der Verarbeitungstätigkeit

Eindeutige Bezeichnung der dokumentierten Verarbeitung/der Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen geläufige Bezeichnung des Fachprozesses gewählt werden.

Empfehlung: Der **Name der Verarbeitung sollte unabhängig von einzelnen IT-Tools** sein, die ggfs. im Rahmen der Verarbeitung/des Prozesses zum Einsatz kommen.

Beispiele:

- >> Allgemeine Kundenverwaltung
- >> Customer-Relationship-Management (CRM)

#### 2. Verantwortlicher Fachbereich/sonstige Zuordnungskennzeichen

Angabe, um unternehmensintern die Zuordnung der dokumentierten Verarbeitungstätigkeit im VVT zu einem bestimmten Fachbereich und dessen erweiterter Dokumentation herstellen zu können.

Dies kann z.B. mittels der Funktionsbezeichnung des Fachbereiches oder eines sonstigen Zuordnungskennzeichens (z.B. eine eindeutige Identifikationsnummer) erfolgen.

#### 3. Bei gemeinsamer Verantwortlichkeit

Falls mehrere Verantwortliche gemeinsam für die Verarbeitungstätigkeiten verantwortlich sind, bspw. innerhalb einer Unternehmensgruppe, sind hier Name und Kontaktdaten (ladungsfähige Anschrift) des oder der weiteren Verantwortlichen anzugeben (Firma/ladungsfähige Anschrift; Art. 30 Abs. 1 lit. a DS-GVO, Art. 26 Abs. 1 DS-GVO).

#### 4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

Beispiele:

- >> Verarbeitungstätigkeit: „Allgemeine Kundenverwaltung“; verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso“
- >> Verarbeitungstätigkeit: „Customer-Relationship-Management“; verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Kundenbeziehungen, Marketing, Neukundenakquise, Kundenbindungsmaßnahmen, Kundenberatung, Beschwerdemanagement, Kündigungsprozess“

Eine Verarbeitungstätigkeit kann mehrere Teil-Geschäftsprozesse (der EuGH spricht von „Vorgängen“) zusammenfassen. Dementsprechend kann eine Verarbeitung auch mehrere Zwecke umfassen, so dass auch mehrere Zweckbestimmungen angegeben werden können.

Die Detailtiefe hängt von der Geschäftstätigkeit des Unternehmens ab.

Es können neben dem Fachprozess auch begleitende mitarbeiterbezogene Unterstützungsprozesse vorliegen, wie z.B. zur Personalführung/-einsatzplanung. Diese können entweder als Teil einer anderen Verarbeitung oder als eigene Verarbeitung beschrieben sein.

#### 5. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)

Als betroffene Personengruppen kommen beispielsweise Kunden, Interessenten, Arbeitnehmer, Schuldner, Versicherungsnehmer usw. in Betracht. Den einzelnen Personengruppen sind die jeweils auf sie bezogenen verwendeten Daten oder Datenkategorien zuzuordnen. Damit sind keine personenbezogenen Daten, sondern „Datenbezeichnungen“/ Datenkategorien gemeint (z.B. „Adresse“, „Geburtsdatum“, „Bankverbindung“). Werden solche Datenkategorien angegeben, so müssen diese so

konkret wie möglich sein. Nicht ausreichend, da zu allgemein, sind etwa Angaben wie „Kundendaten“ oder Ähnliches.

Beispiele:

- >> Kunden: Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax- und E-Mail-Daten), Geburtsdatum, Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließl. Kundenentwicklung, Produkt- bzw. Vertragsinteresse, Statistikdaten, Abrechnungs- und Leistungsdaten, Bankverbindung
- >> Beschäftigtendaten (Lohn und Gehalt): Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, etc.

#### 6. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden (Art. 30 Abs. 1 lit. d DS-GVO)

Empfängerkategorien sind insbesondere am Prozess beteiligte weitere Stellen des Unternehmens/ Konzerns oder andere Gruppen von Personen oder Stellen, die Daten – ggf. über Schnittstellen – erhalten; z.B. in den Prozess eingebundene weitere Fachabteilungen, Vertragspartner, Kunden, Behörden, Versicherungen, Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.

Die Angaben können als Kategorien aus den detaillierteren Angaben unter Pkt. 17/18 übernommen werden.

#### 7. Datenübermittlungen in Drittländer oder internationale Organisationen (Art. 30 Abs. 1 lit. e DS-GVO)

Es sind hier Datenübermittlungen in Drittländer oder an internationale Organisationen anzugeben. Drittländer sind solche außerhalb der EU/des EWR. Beispiele für internationale Organisationen: Institutionen der UNO, der EU.

Es ist die Angabe des betreffenden Drittlandes erforderlich.

Lediglich in Ausnahmefällen wird es erforderlich sein, Angaben zu geeigneten Garantien anzugeben: nämlich dann, wenn keine der genannten Garantien vorliegt, sind hier andere getroffene Garantien zu dokumentieren (Art. 49 Abs. 1. UAbs. 2 DS-GVO)<sup>18</sup>. Falls es sich bspw. um ein Drittland mit Angemessenheitsbeschluss der EU-Kommission handelt, EU-Standarddatenschutzklauseln abgeschlossen wurden, oder verbindliche interne Datenschutzvorschriften vorliegen, sind nähere Angaben zu den Garantien nicht erforderlich.

Detailliertere Angaben zu internen Nachweiszwecken erfolgen unter Pkt. 19.

## 8. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 lit. f DS-GVO)

Anzugeben sind hier die konkreten Aufbewahrungs-/Löschfristen, die in Verarbeitungstätigkeiten implementiert sind. Falls für einzelne Verarbeitungsschritte, unterschiedliche Fristen gelten, ist dies jeweils zu dokumentieren.

Soweit die Fristen in einem Löschkonzept dokumentiert sind, reicht der konkrete Verweis auf dieses vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.

## 9. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i. V. m. Art. 32 Abs. 1 DS-GVO)

- >> Soweit für die Verarbeitung die Vorgaben des übergreifenden Sicherheitskonzepts (**siehe Vorblatt 2 Nr. 5**) Anwendung finden, kann hierauf verwiesen werden. Eventuelle Abweichungen sind zusätzlich zum Verweis zu dokumentieren.
- >> Soweit sich die technischen und organisatorischen Maßnahmen aus anderen vorhandenen Sicherheitsrichtlinien/Konzepten/Zertifizierungen, z.B. aus dem Sicherheitskonzept eines eingebundenen Auftragsverarbeiters, ergeben, ist ein konkreter Verweis hierauf ausreichend. Eventuelle Abweichungen sind zusätzlich zum Verweis zu dokumentieren.
- >> Soweit für die technischen und organisatorischen Maßnahmen keine der vorgenannten Dokumentationen vorliegen, sind sie hier im Einzelnen zu dokumentieren.

Ein Verweis auf das Vorhandensein einer Datenschutz-Folgenabschätzung ist eine sinnvolle optionale Angabe, um darüber aufzuzeigen, dass eine individuelle Betrachtung der Risiken erfolgt ist und

---

<sup>18</sup> Dies betrifft nur folgenden Ausnahmefall:

- Die Übermittlung kann nicht auf
  - > eine Bestimmung der Art. 45 oder 46 – einschließlich der verbindlichen internen Datenschutzvorschriften oder
  - > eine der Ausnahmen für einen bestimmten Fall gemäß Art. 49 Abs. 1 Satz 1 Buchstaben a bis ggestützt werden und folgende Bedingungen sind alle erfüllt:
  - > die Übermittlung erfolgt nicht wiederholt,
  - > betrifft nur eine begrenzte Zahl von betroffenen Personen,
  - > ist für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen,
  - > der Verantwortliche hat alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung angemessene Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen,
  - > der Verantwortliche hat die Aufsichtsbehörde von der Übermittlung in Kenntnis gesetzt und
  - > der Verantwortliche hat die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen unterrichtet.



angemessene Sicherheitsvorkehrungen ergriffen und dokumentiert wurden.

## Weitergehende Angaben zur Verarbeitung zur Erfüllung der Rechenschaftspflichten gem. Art. 5 (2) DS-GVO

### 10. Datum und Art der Meldung

Es ist das Datum anzugeben, an dem die Verarbeitungsmeldung ausgefüllt wurde.

Es ist darüber hinaus anzugeben, ob es sich um die Meldung einer neuen Verarbeitung handelt, oder um die Änderung oder Löschung einer bestehenden Verarbeitung.

### 11. Geplanter Beginn der Verarbeitung von personenbezogenen Daten oder tatsächlicher Beginn

Dabei ist schon die erstmalige Übertragung oder Speicherung von personenbezogenen Daten relevant.

### 12. Wesentliche Prozessschritte

Hiermit ist eine Übersicht über die einzelnen Verarbeitungsschritte gemeint, z.B. in chronologischer Form. Es kann auch auf Datenflussdiagramme o.ä. verwiesen werden (siehe Pkt. 13).

Beispiel:

- >> Erstellung von werblichen Briefen an Kunden durch Vertrieb
  - a. Auswahl Kunden und Anschriften
  - b. Weiterleitung Kundenanschriften an Dienstleister (Auftragsverarbeitung)
  - c. Druck und Versand incl. Werbematerial durch Dienstleister
- >> Löschen der Kundendaten beim Dienstleister

### 13. Ergänzende Dokumente und Unterlagen

Hier sollten ggfs. relevante Datenflusspläne, Handbücher, Lasten-, Pflichtenhefte, Produktbeschreibungen, Internet-Adressen zu Produkten, Angaben zu Datenquellen und Schnittstellen etc. beigelegt oder verlinkt werden.

### 14. Verarbeitung von besonderen Kategorien personenbezogener Daten

Hier sollte noch einmal gesondert dargestellt werden, ob in der Verarbeitungstätigkeit besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO) oder Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO) verarbeitet werden.

### 15. Rechtsgrundlage der Verarbeitungstätigkeit

Bei Unklarheiten sollte dieser Punkt in Abstimmung mit dem Datenschutzbeauftragten oder anderen Mitarbeitern der Datenschutzorganisation gemeinsam ausgefüllt werden.

Insbesondere wichtig ist jedoch die Information seitens des Fachbereiches, ob es **spezialgesetzliche Regelungen** gibt, in denen die Verarbeitung personenbezogener Daten geregelt wird.

Die zutreffende Rechtsgrundlage sollte angekreuzt und erläutert werden. Es können innerhalb einer Verarbeitungsmeldung auch mehrere Rechtsgrundlagen für unterschiedliche Daten oder Verarbeitungsschritte zutreffen.

- >> Spezialgesetzliche Regelung außerhalb der DS-GVO: Benennung von Vorschrift, Paragraph, Absatz, Satz.
- >> Einwilligung des Betroffenen (Art. 6 Abs. 1a DS-GVO): Erläuterung der Einwilligungsklausel und des Einwilligungsmechanismus
- >> Kollektivvereinbarung (z.B. Betriebsvereinbarung, Tarifvertrag): Benennung der Vereinbarung, Paragraph, ggfs. Absatz
- >> Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses
- >> Vertrag oder Vertragsanbahnung mit dem Betroffenen (Art. 6 Abs. 1b DS-GVO)

- >> Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1f DS-GVO): Benennung der berechtigten Interessen.
- >> Sonstiges (bspw. Art. 6 Abs. 1d und e DS-GVO)

## 16. Weitere Angaben bei gemeinsamer Verantwortlichkeit gem. Art. 26 DS-GVO

Falls eine gemeinsame Verantwortlichkeit vorliegt, sollten hier weitere Angaben gemacht werden.

So ist darzulegen, auf welche Vorgänge innerhalb der Verarbeitungstätigkeit sich die gemeinsame Verantwortlichkeit bezieht. Darüber hinaus sollten die Verträge zur gemeinsamen Verantwortlichkeit hier einsehbar/abrufbar sein, und es sollten Angaben zur Erfüllung der Informationspflichten, sowie weiterer relevanter Aspekte im Einzelfall (z.B. zur Erfüllung der Betroffenenrechte) gemacht werden.

## 17. Empfänger, denen die Daten offengelegt worden sind oder noch offengelegt werden

Es sind getrennt alle Stellen im Unternehmen und außerhalb des Unternehmens anzugeben, die **regelmäßig** (= organisatorisch vorgesehen) personenbezogene Daten erhalten. Ob es sich um schriftliche oder IT-technische Datenweitergabe handelt, ist nicht entscheidend.

Es werden hier folgende Empfänger unterschieden:

- >> **Empfänger innerhalb des Verantwortlichen:** z.B. Abteilungen innerhalb des Unternehmens, die Daten im Rahmen der Verarbeitung erhalten. Z.B. an die Tax-Abteilung, Personalabteilung etc.
- >> **Empfänger (Dritte) außerhalb des Verantwortlichen:** Empfänger, die nicht zum Verantwortlichen gehören (andere Konzerngesellschaften, Gesellschaften außerhalb des Kon-

zerns, Kooperationspartner, Geschäftspartner) und denen regelmäßig personenbezogene Daten im Rahmen der Verarbeitung übermittelt werden.

Die hier dokumentierten Empfänger werden dabei jeweils einer Kategorie zugeordnet. Diese Kategorien sind in einer Liste unter Pkt. 6 aufzuführen und stellen darüber hinaus eine relevante Angabe für die Datenschutzinformation dar.

Mittels **Auftragsverarbeitung beauftragte Dienstleister**, die Daten im Rahmen der Verarbeitung erhalten (z.B. Callcenter, Druckdienstleister) sind unter Pkt. 18 aufzuführen.

## 18. Eingebundene Dienstleister

Werden Dienstleister beauftragt, für den Verantwortlichen Leistungen auszuführen, die mit der Verarbeitung von personenbezogenen Daten einhergehen, dann sind diese hier zu benennen.

Es ist jeweils anzugeben, ob es sich um eine Auftragsverarbeitung gem. Art. 28 DS-GVO handelt, und ggfs. die entsprechenden vertraglichen Vereinbarungen beizufügen oder zu verlinken.

## 19. Garantien im Falle von Datenübermittlungen in Drittländer oder internationale Organisationen (vgl. Nr. 7, Nr. 17, Nr. 18)

Im Falle von Datenweitergaben außerhalb von EU/EWR sind geeignete Garantien beim Empfänger grundsätzlich erforderlich und hier anzugeben, falls für das betreffende Land kein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DS-GVO vorliegt. Solche Garantien können gem. Art. 46 DS-GVO durch verbindliche interne Datenschutzvorschriften (BCR) oder EU-Standardvertragsklauseln erbracht werden.

Darüber hinaus müssen hier – falls die Datenübermittlungen nicht auf anderem Wege (wie in Art. 45-47 DS-GVO beschrieben) abgesichert sind –

geeignete Garantien bei Datenübermittlungen auf der Grundlage von Art. 49 Abs. 1 UAbs. 2 DS-GVO angegeben werden.<sup>19</sup>

## 20. Beteiligte IT-Systeme

An dieser Stelle sollte eine knappe Beschreibung der technischen Infrastruktur angegeben werden, um ein besseres Verständnis der allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen zu ermöglichen.

Darüber hinaus kann die Beschreibung zur Identifikation von Dienstleistern mit Auftragsverarbeitungs-Relevanz dienen (vgl. Pkt. 18).

Falls personenbezogene Daten auch in Nicht-Produktivsystemen verarbeitet werden, sollten hier entsprechende Angaben zur Rechtmäßigkeit sowie zu Schutzmaßnahmen gemacht werden.

## 21. Wie und zu welchem Zeitpunkt werden die Informationspflichten erfüllt?

Hier ist zu dokumentieren, wie die Informationspflichten nach Art. 12-14 DS-GVO erfüllt werden.

## 22. Wird die Verarbeitung auch dienstleistend für weitere Unternehmen durchgeführt?

Wenn diese Verarbeitung (auch) dienstleistend für andere Auftraggeber-Gesellschaften in Form einer Auftragsverarbeitung durchgeführt wird, dann ist dies mittels eines Vertrages zur Auftragsverarbeitung (in der Rolle des Dienstleisters) abzusichern und im sog. „Verzeichnis von Verarbeitungstätigkeiten des Auftragsverarbeiters“ (VVT-AV, vgl. Praxishilfe Vb der GDD) des Unternehmens zu dokumentieren.

## 23. Wie sind die Zugriffsberechtigungen geregelt?

Diese Dokumentation dient als Nachweis, dass die Vertraulichkeit der Daten gewährleistet ist, indem Berechtigungen nur im erforderlichen Umfang vergeben werden, und die vergebenen Berechtigungen stets richtig und aktuell sind.

Es sind alle Personengruppen anzugeben, die eine Berechtigung haben, die Daten zu lesen oder zu verändern (Rollen-, Berechtigungskonzept), sowie der Prozess zur Erlangung und Verwaltung der Berechtigungen.

---

<sup>19</sup> Dies betrifft nur folgenden Ausnahmefall:

- Die Übermittlung kann nicht
  - > auf eine Bestimmung der Art. 45 oder 46 – einschließlich der verbindlichen internen Datenschutzvorschriften
  - > auf eine der Ausnahmen für einen bestimmten Fall gemäß Art. 49 Abs. 1 Satz. 1 Buchstaben a bis g gestützt werden und folgende Bedingungen sind alle erfüllt:
    - > die Übermittlung erfolgt nicht wiederholt,
    - > betrifft nur eine begrenzte Zahl von betroffenen Personen,
    - > ist für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen,
    - > der Verantwortliche hat alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung angemessene Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen,
    - > der Verantwortliche hat die Aufsichtsbehörde von der Übermittlung in Kenntnis gesetzt und
    - > der Verantwortliche hat die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen unterrichtet.

## 24. Angaben zum Umfang der Verarbeitung

Die DS-GVO fordert an mehreren Stellen die Berücksichtigung des Umfanges der Verarbeitung (bspw. hinsichtlich der Bewertung der Angemessenheit der Sicherheitsmaßnahmen, oder der Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung).

Rechtsverbindliche Angaben zu Schwellenwerten für einen „großen Umfang der Verarbeitung“ liegen bislang allerdings nicht vor.

## 25. Risiko der Verarbeitung und Datenschutz-Folgenabschätzung

Das von der DS-GVO geforderte „risikoorientierte“ Vorgehen setzt voraus, dass eine Transparenz über das Risiko der einzelnen Verarbeitungen im Unternehmen vorliegt. Daher ist es geboten, jede Verarbeitung hinsichtlich des Datenschutz-Risikos zu bewerten, und – im Falle des Vorliegens eines hohen Risikos – ggfs. eine Datenschutz-Folgenabschätzung durchzuführen.

Siehe hierzu auch: GDD-Praxishilfe DS-GVO – Voraussetzungen der Datenschutz-Folgenabschätzung.

## 26. Wahrung der (weiteren) Betroffenenrechte

Hier sollten ggfs. relevante Angaben gemacht werden, wie die Wahrnehmung der unterschiedlichen weiteren Betroffenenrechte (Recht auf Auskunft, Berichtigung, Einschränkung, Widerspruch, Datenübertragbarkeit sowie im Zusammenhang mit automatisierten Entscheidungen im Einzelfall einschließlich Profiling) ermöglicht wird.

## 27. Wie wird der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sichergestellt?

Hier sollten entsprechende Beschreibungen oder auch selbst erarbeitete Checklisten eingebettet werden, um den Nachweis zu erbringen, dass die Verarbeitung in Einklang mit Art. 25 DS-GVO erfolgt.

## 7. Anlage Muster zum VVT von EU-Aufsichtsbehörden

Aufsichtsbehörde (Staat)	Hinweise	Muster	Link	Hyperlink
Deutschland				
>> DSK			<a href="https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf">https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf</a>	<a href="#">aufrufen</a>
			<a href="https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf">https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf</a>	<a href="#">aufrufen</a>
>> LDA Bayern			<a href="https://www.lda.bayern.de/de/muster.html">https://www.lda.bayern.de/de/muster.html</a>	<a href="#">aufrufen</a>
			<a href="https://www.lda.bayern.de/media/muster/muster_5_arztpraxis_verzeichnis.pdf">https://www.lda.bayern.de/media/muster/muster_5_arztpraxis_verzeichnis.pdf</a>	<a href="#">aufrufen</a>
			<a href="https://www.lda.bayern.de/media/muster/muster_11_behoerungsbetrieb_verzeichnis.pdf">https://www.lda.bayern.de/media/muster/muster_11_behoerungsbetrieb_verzeichnis.pdf</a>	<a href="#">aufrufen</a>
			<a href="https://www.lda.bayern.de/media/muster/muster_12_einzelhaendler_verzeichnis.pdf">https://www.lda.bayern.de/media/muster/muster_12_einzelhaendler_verzeichnis.pdf</a>	<a href="#">aufrufen</a>
			<a href="https://www.lda.bayern.de/media/muster/muster_2_kfz-werkstatt_verzeichnis.pdf">https://www.lda.bayern.de/media/muster/muster_2_kfz-werkstatt_verzeichnis.pdf</a>	<a href="#">aufrufen</a>
			<a href="https://www.lda.bayern.de/media/muster/muster_9_online-shop_verzeichnis.pdf">https://www.lda.bayern.de/media/muster/muster_9_online-shop_verzeichnis.pdf</a>	<a href="#">aufrufen</a>
			<a href="https://www.lda.bayern.de/media/muster/muster_1_verein_verzeichnis.pdf">https://www.lda.bayern.de/media/muster/muster_1_verein_verzeichnis.pdf</a>	<a href="#">aufrufen</a>
			<a href="https://www.lda.bayern.de/media/muster/muster_6_weg-verwaltung_verzeichnis.pdf">https://www.lda.bayern.de/media/muster/muster_6_weg-verwaltung_verzeichnis.pdf</a>	<a href="#">aufrufen</a>
Belgien			<a href="https://www.autoriteprotectiondonnees.be/canevas-de-registre-des-activites-de-traitement">https://www.autoriteprotectiondonnees.be/canevas-de-registre-des-activites-de-traitement</a>	<a href="#">aufrufen</a>
			<a href="https://www.autoriteprotectiondonnees.be/node/20442">https://www.autoriteprotectiondonnees.be/node/20442</a> auch unter <a href="https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/canevas%20registre%20des%20activites%20de%20traitement_version_19072017.xls">https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/canevas%20registre%20des%20activites%20de%20traitement_version_19072017.xls</a>	<a href="#">aufrufen</a> <a href="#">aufrufen</a>
Dänemark			<a href="https://www.datatilsynet.dk/media/6567/fortegnelse.pdf">https://www.datatilsynet.dk/media/6567/fortegnelse.pdf</a>	<a href="#">aufrufen</a>
Finland			<a href="https://tietosuoja.fi/en/record-of-processing-activities">https://tietosuoja.fi/en/record-of-processing-activities</a>	<a href="#">aufrufen</a>
			<a href="https://tietosuoja.fi/en/controller-s-record-of-processing-activities">https://tietosuoja.fi/en/controller-s-record-of-processing-activities</a>	<a href="#">aufrufen</a>
			<a href="https://tietosuoja.fi/documents/6927448/8323207/Template+for+controllers+-+record+of+processing+activities.xlsx/696390cb-00ae-4780-884a-668d0f8dd655">https://tietosuoja.fi/documents/6927448/8323207/Template+for+controllers+-+record+of+processing+activities.xlsx/696390cb-00ae-4780-884a-668d0f8dd655</a>	<a href="#">aufrufen</a>
Frankreich			<a href="https://www.cnil.fr/fr/cartographie-vos-traitements-de-donnees-personnelles">https://www.cnil.fr/fr/cartographie-vos-traitements-de-donnees-personnelles</a>	<a href="#">aufrufen</a>
			<a href="https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement">https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement</a>	<a href="#">aufrufen</a>
			<a href="https://www.cnil.fr/sites/default/files/atoms/files/registre-traitement-simplifie.ods">https://www.cnil.fr/sites/default/files/atoms/files/registre-traitement-simplifie.ods</a>	<a href="#">aufrufen</a>

Aufsichtsbehörde (Staat)	Hinweise	Muster	Link	Hyperlink
Griechenland			<a href="https://www.dpa.gr/portal/page?_pageid=33,211400&amp;dad=portal&amp;_schema=PORTAL">https://www.dpa.gr/portal/page?_pageid=33,211400&amp;dad=portal&amp;_schema=PORTAL</a>	<a href="#">aufrufen</a>
			<a href="http://www.dpa.gr/pls/portal/url/ITEM/6CDCE1FFFC42A14AE050A8C07C243BD0">http://www.dpa.gr/pls/portal/url/ITEM/6CDCE1FFFC42A14AE050A8C07C243BD0</a>	<a href="#">aufrufen</a>
Großbritannien			<a href="https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/#how5">https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/#how5</a>	<a href="#">aufrufen</a>
			<a href="https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx">https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx</a>	<a href="#">aufrufen</a>
Italien			<a href="https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento">https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento</a>	<a href="#">aufrufen</a>
			<a href="https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048342">https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048342</a>	<a href="#">aufrufen</a>
			<a href="https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048327">https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048327</a>	<a href="#">aufrufen</a>
			<a href="https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048348">https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048348</a>	<a href="#">aufrufen</a>
		<a href="https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048395">https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048395</a>	<a href="#">aufrufen</a>	
Liechtenstein			<a href="https://www.datenschutzstelle.li/index.php?cID=319">https://www.datenschutzstelle.li/index.php?cID=319</a>	<a href="#">aufrufen</a>
			<a href="https://www.datenschutzstelle.li/download_file/300/319">https://www.datenschutzstelle.li/download_file/300/319</a>	<a href="#">aufrufen</a>
Luxemburg			<a href="https://cnpd.public.lu/en/professionnels/obligations/registre.html">https://cnpd.public.lu/en/professionnels/obligations/registre.html</a>	<a href="#">aufrufen</a>
	*	*	<a href="https://cst.cnpd.lu/portal/">https://cst.cnpd.lu/portal/</a>	<a href="#">aufrufen</a>
Polen			<a href="https://uodo.gov.pl/pl/file/708">https://uodo.gov.pl/pl/file/708</a>	<a href="#">aufrufen</a>
Spanien			<a href="https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/actividades-tratamiento">https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/actividades-tratamiento</a>	<a href="#">aufrufen</a>
			<a href="https://www.aepd.es/es/prensa-y-comunicacion/blog/elaborar-el-registro-de-actividades-de-tratamiento">https://www.aepd.es/es/prensa-y-comunicacion/blog/elaborar-el-registro-de-actividades-de-tratamiento</a>	<a href="#">aufrufen</a>

\* "GDPR Compliance Support Tool" mit der Möglichkeit, das VVT hier anzulegen

**Auf den Webseiten folgender Aufsichtsbehörden konnten keine Hinweise oder Muster zur Führung eines VVT gefunden werden:**

>> **Bulgarien**

>> **Estland**

>> **Irland**

>> **Österreich** (allerdings Verweis auf Bundesministerium für Digitalisierung und Wirtschaftsstandort:

[https://www.usp.gv.at/Portal.Node/usp/public/content/it\\_und\\_geistiges\\_eigentum/datenschutz\\_neu/datenverarbeitungsverzeichnis/313018.html](https://www.usp.gv.at/Portal.Node/usp/public/content/it_und_geistiges_eigentum/datenschutz_neu/datenverarbeitungsverzeichnis/313018.html)

aufrufen

<https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Dokumentationspflicht.htm>

aufrufen

<https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Verantwortlicher.docx>

aufrufen

>> **Niederlande**

>> **Schweden**

>> **Schweiz**

*[Stand 17.01.2020; bei weiteren Aufsichtsbehörden der EU/des EWR wurde nicht gesucht]*



Gesellschaft für Datenschutz  
und Datensicherheit e.V.

## Mitglied werden? Mehr Informationen?

<https://www.gdd.de/service/mitglied-werden> oder eine E-Mail an: [info@gdd.de](mailto:info@gdd.de)

### **Eine Mitgliedschaft bietet wesentliche Vorteile:**

- >> Mitglieder-Nachrichten mit aktuellen Fachinformationen
- >> Bezug der Fachzeitschrift RDV (Recht der Datenverarbeitung)
- >> Beratung bei konkreten Einzelfragen
- >> Zugriff auf Rechtsprechungs- und Literaturarchiv
- >> Online-Service „DataAgenda Plus“ (Muster, Checklisten, RDV ONLINE Archiv, Arbeitspapiere etc.)
- >> Mitarbeit in Erfahrungsaustausch- und Arbeitskreisen
- >> Teilnahme an den kostenfreien GDD-Informationstagen sowie Vergünstigungen bei Seminaren u.v.m.

Schließen Sie sich unseren mehr als 3.800 Mitgliedern an. Eine Mitgliedschaft erhalten Sie schon ab 150,- EUR/Jahr für Privatpersonen und ab 300,- EUR/Jahr für Firmen.

---

### **Herausgeber:**

Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

Heinrich-Böll-Ring 10

53119 Bonn

Tel.: +49 228 96 96 75-00

Fax: +49 228 96 96 75-25

[www.gdd.de](http://www.gdd.de)

[info@gdd.de](mailto:info@gdd.de)

Satz: C. Wengenroth, GDD-Geschäftsstelle

### **Ansprechpartner:**

RA Steffen Weiß, LL.M.

### **Stand:**

Version 2.2 (Juli 2022)