Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO V

Verzeichnis von Verarbeitungstätigkeiten

INHALT

1. Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche

1.1 Prämissen 4
1.2 Inhalte 6
1.3 Muster 6

2. Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter

2.1 Prämissen 12
2.2 Inhalte 14
2.3 Aufbau 14

3. Verzeichnis von Verarbeitungstätigkeiten für Vertreter in der EU 16

Verzeichnis von Verarbeitungstätigkeiten

Aus dem Verfahrensverzeichnis bzw. der Verarbeitungsübersicht gemäß der §§ 4e und 4g BDSG/Artt. 18, 19 RL 95/46/EG wird künftig das Verzeichnis Verarbeitungstätigkeiten (VVT) gemäß Art. 30 DS-GVO. Nach Erwägungsgrund 82 der DS-GVO soll der Verantwortliche „zum Nachweis der Einhaltung dieser Verordnung" das Verzeichnis von Verarbeitungstätigkeiten führen. Weiterhin kann die zuständige Aufsichtsbehörde die Vorlage verlangen, um die betreffenden Stellen hoheitlich zu kontrollieren.

Bestehende Verarbeitungsübersichten nach den §§ 4e und 4g BDSG sind eine gute Grundlage für das VVT – müssen aber unter der DS-GVO angepasst werden.[1]

1 BayLDA, Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO, Positionspapier Nr. 5 vom 02.08.2016.

1. Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche

1.1 Prämissen

1.1.1 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; oder
- >> mit einem besonderem Risiko bei der Verarbeitung; oder
- >> mit Verarbeitung von sensiblen Daten (Artt. 9 und 10 DS-GVO); oder
- >> einer nicht nur gelegentlichen Verarbeitung.

Allerdings geht diese Ausnahmeregelung ins Leere. Spätestens bei Zugrundelegung einer regelmäßigen Verarbeitung sind sämtliche Verantwortlichen unabhängig von ihrer Mitarbeiterstärke betroffen.

Trotz des verunglückten Wortlauts des Art. 30 Abs. 5 DS-GVO in der ursprünglichen amtlichen deutschen Übersetzung genügt es nicht, dass nur einer der privilegierenden Tatbestände vorliegt, um auf ein VVT verzichten zu dürfen.[2] Die Übersetzung wurde inzwischen korrigiert.[3]

Auftragsverarbeiter müssen gem. Art. 30 Abs. 2 DS-GVO explizit ein Verzeichnis im Hinblick auf ihre Dienstleistung führen (VVT-AV). Dies entbindet allerdings nicht von der Verpflichtung zu einem originären VVT nach Art. 30 Abs. 1 DS-GVO für die eigenen Geschäftsprozesse. In der Praxis erscheint es sinnvoll, gesonderte Vorlagen für die allgemeinen Verarbeitungen des Unternehmens sowie für den Bereich der Auftragsverarbeitung zu haben (jeweils mit eigenem Aufbau und als gesonderte Formulare).

1.1.2 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.

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 eventuell federführend wird.[4]

Die Trennung in ein internes und ein externes Verzeichnis „für Jedermann“ ist in der DS-GVO nicht mehr vorgesehen. Das VVT steht nur für interne Zwecken und auf Anfrage der zuständigen Auf-

2 Martini in: Paal/Pauly, DS-GVO, 2017, Art. 30 Rn. 30 f.
3 Drucksache vom 27.10.2016, http://data.consilium.europa.eu/doc/document/ST-12399-2016-INIT/en/pdf.
4 Das BayLDA geht derzeit 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.

sichtsbehörde zur Verfügung. Ein „öffentliches Verfahrensverzeichnis“ wird nicht mehr benötigt. Seine Pflege und Bereithaltung kann ab 25.5.2018 eingestellt werden. Die nach BDSG vorgesehene Trennung nach unterschiedlichen Informationen für den Datenschutzbeauftragten und die Aufsichtsbehörden (Übersicht zugriffsberechtigter Personen nach § 4g Abs. 2 Satz 1 BDSG) entfällt ebenfalls.

1.1.3 Zentrale Führung und weitergehende Dokumentationspflichten

Im Gegensatz zum Verfahrensverzeichnis nach BDSG ist das VVT nicht an den Datenschutzbeauftragten zu übergeben, sondern unmittelbar vom Verantwortlichen zu führen. Es mag naheliegen, das Verzeichnis zentral führen zu wollen. Auch die Art.-29-Datenschutzgruppe erachtet es für zulässig, den DSB mit der Erstellung/Führung/Pflege zu betrauen,[5] doch es muss stets klar sein, dass das Verzeichnis der Verantwortung des Unternehmens obliegt. Die Angaben zum Verzeichnis sind durch das Unternehmen bzw. – im Wege der Delegation – die Fachbereiche beizubringen.

Im Sinne einer „best practice“ erscheint es dann sinnvoll, dass das Verzeichnis als Dreh- und Angelpunkt des gesamten Datenschutzmanagements vom DSB geführt wird. Mit Blick auf die weitergehenden Accountability-Pflichten der DS-GVO avanciert das VVT zum zentralen Bestandteil der Dokumentation. Das VVT kann beispielsweise zur Grundlage für Risikobewertungen durch den DSB für dessen risikoorientierten Überwachungsauftrag werden (Art. 39 Abs. 2 DS-GVO). Ohne eine solche strukturierte Dokumentation sind die Beratungs- und Kontrollpflichten des DSB kaum umsetzbar.

Denkbar sind interne Erweiterungen des VVT durch Risikoabschätzungen bzw. eine zusätzliche Strukturierung, die festhält, welche Verarbeitungen ggf. eine Datenschutz-Folgenabschätzung erfordern und welche nicht. Daneben können die durchgeführten Prüfungen aufgenommen werden.

Aber: Das VVT darf nicht nicht überfrachtet werden! Es wirkt kontraproduktiv, das VVT zu sehr aufzublähen. Es sollte beispielsweise von der allgemeinen Informationssicherheit und ihren Übersichten klar getrennt sein. Besser ist es, die getroffenen technisch-organisatorischen Maßnahmen (TOMs) konkret dort aufzunehmen, wo ein Verweis auf die von der IT geführte Dokumentation nicht ausreicht.

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

1.1.4 Drittlandstransfers

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 und 2 DS-GVO zu dokumentieren. Die auf diese Regelung gestützten Weitergaben erfolgen nicht wiederholt. Die zu dokumentierenden Prozesse sind hingegen gerade auf Wiederholung angelegt.

5 Artikel-29-Gruppe, WP 243 Guidelines on Data Protection Officers (rev. 1) vom 5.4.2017, http://ec.europa.eu/newsroom/document.cfm?doc_id=44100.

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

1.2 Inhalte

Das VVT ist – wie früher das Verfahrensverzeichnis nach dem BDSG – nicht als Auflistung einzelner Verarbeitungen, sondern als prozessorientierte Übersicht der Verarbeitungen zu verstehen. Das Verständnis des Verfahrensbegriffs als Bündel von Verarbeitungsschritten, wie es in Art. 18 Abs. 1 RL 95/46/EG niedergelegt war, lebt insoweit fort. Entscheidend ist, 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:

- 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;
- gegebenenfalls 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 Dokumentierung 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 litt. f und g DS-GVO: Es wird erwartet, dass diese Informationen vorliegen.

1.3 Muster

Die optionalen Angaben werden gesetzlich nicht zur Dokumentation im VVT gefordert. Dennoch kann die Dokumentation der Angaben im VVT geboten sein, da sie zur Erfüllung der Nachweispflichten i. S. d. Art. 5, 24 DS-GVO beitragen.

1.3.1 Hauptblatt

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Hauptblatt

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

1. Verantwortlicher (= Firma / 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

Optionale Inhalte / Übergreifende Regelungen und Sachverhalte

5. Zuständige Aufsichtsbehörde

Name

Die zuständige Aufsichtsbehörde aus Sicht des verantwortlichen. Mitunter kann eine andere Behörde federführend sein, auch dieser ist auf Anfrage das VVT zur Verfügung zu stellen.

Meldung des/der Datenschutzbeauftragten erfolgt:

☐ Ja
☐ Nein

6. Regelungen zur Datensicherheit

Verweis auf übergreifende IT-Sicherheitskonzepte, die grunds. für alle Verarbeitungstätigkeiten gelten

7. Regelungen zur Datenlöschung

Verweis auf übergreifende Löschkonzepte, die grunds. für alle Verarbeitungstätigkeiten gelten

8. Sachverhalte zu Drittstaatenübermittlungen

Verweis auf übergreifende Punkte wie BCR, die grunds. für alle Verarbeitungstätigkeiten gelten

Erläuterungen

Nr. 1

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

Nr. 2

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-Impressum eingetragen werden.

Nr. 3

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.

Nr. 4

Vom Verantwortlichen bestellter Datenschutzbeauftragter* [Name, Kontaktdaten

Nr. 5

Die Meldung der Kontakt-Informationen des DSB – z.B. (Funktions-)e-mail-Adresse, Telefonnummer – ist verpflichtend.

Nr. 6

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 ISMS nach ISO27001.

Nr. 7

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

Nr. 8

Ein Verweis Regelungen zur Drittstaatenübermittlung sind hier sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen hierdurch geregelt werden, z.B. durch BCR.

1.3.2 Anlage

Verzeichnis von Verarbeitungstätigkeiten Anlage Nr. _____

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

1. Bezeichnung der Verarbeitungstätigkeit

2. Verantwortlicher Fachbereich/verantwortliche Führungskraft (optionaler Inhalt)

3. Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen

Angaben zur Verarbeitungstätigkeit

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit

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

6.1 Betroffene Personengruppen	6.2 Kategorien personenbezogener Daten

7. 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

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

8. 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)

Optionale Angaben

Ggf. vereinbarte Garantien

☐ Anerkannter Drittstaat
☐ EU-Standardvertrag C/C
☐ EU-Standardvertrag C/P
☐ Aufsichtsbehördlich genehmigter Vertrag
☐ BCR
☐ Andere:

Ende optionale Angaben

Garantien zum Schutz der personenbezogenen Daten im Drittland, soweit weder eine Anerkennung des Datenschutzniveaus, EU-Standardverträge noch BCR vorliegen:

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

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

10.1 Art der eingesetzten DV-Anlagen und Software (optional)

>> DV-Anlagen
>> Software (und ggf. Unterprogramme)
>> Schnittstellen

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

>> Bezug zum IT-Sicherheitskonzept, Abweichungen bzw. Ergänzungen
  > *oder:* Link auf TOM (Processor) hier anführen
  > *oder:* Verweis auf Datenschutz-Zertifizierung etc.

Optionale Angaben

>> Zu Informationspflichten
>> Zu Verträgen mit Dienstleistern
>> Zu Vereinbarungen zur gemeinsamen Verantwortung
>> Zu durchgeführten Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten

Ende optionale Angaben

Erläuterungen

Nr. 1

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

Beispiele:

>> Allgemeine Kundenverwaltung

>> Customer-Relationship-Management (CRM)

Nr. 2

Nach der Unternehmensorganisation für die konkrete Verarbeitungstätigkeit verantwortlicher Fachbereich/verantwortliche Führungskraft *(sofern möglich und sinnvoll, zumindest als Funktionsbezeichnung)*

Nr. 3

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

Nr. 4

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 (aus der Anwendung des BDSG als „Verfahren" vertraut) kann mehrere Teil-Geschäftsprozesse zusammenfassen. Dementsprechend kann eine Verarbeitung auch mehrere Zwecke umfassen, so dass auch mehrere Zweckbestimmungen angegeben werden können.

Die erforderliche Detailtiefe hängt von der Geschäftstätigkeit des Verantwortlichen 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.

Nr. 5

Die Nennung der einschlägigen Rechtsgrundlage ist für Accountability-Pflichten und die Gewährleistung von transparenzpflichten ggü. betroffenen Personen notwendig.

Nr. 6

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

Nr. 6.1

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

Nr. 6.2

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.

Nr. 7

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.

Nr. 8

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

>> Geeignete Garantien beim Empfänger sind grds. erforderlich, falls für den 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-Standardverträge erbracht werden.

Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren (Art. 49 Abs. 1. UAbs. 2 DS-GVO)

Nr. 9

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.

Nr. 10

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

Nr. 10.1

Optional kann an dieser Stelle eine knappe Beschreibung der technischen Infrastruktur wie der technischen und organisatorischen Sicherheitsmaßnahmen angegeben werden, um ein besseres Verständnis der allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen (siehe 10.2.) zu ermöglichen.

Nr. 10.2

Soweit sich die technischen und organisatorischen Maßnahmen schon aus vorhandenen Sicherheitsrichtlinien/Konzepten/Zertifizierungen ergeben, ist ein konkreter Verweis hierauf ausreichend. Insbesondere sind hier Abweichungen zu einem übergrei-

fenden Sicherheitskonzept (siehe Hauptblatt Nr. 6) zu dokumentieren. Wenn eine Datenschutz-Folgenabschätzung für die Verarbeitung hohe Risiken ausweist, so sind die zur Bewältigung dieser Risiken getroffenen Sicherheitsvorkehrungen für die Verarbeitung in der Datenschutz-Folgenabschätzung zu dokumentieren. (Art. 35 Abs. 7 lit. d DS-GVO). Ein Verweis auf das Vorhandensein einer Datenschutz-Folgenabschätzung ist eine sinnvolle optionale Angabe (siehe unten).

Nr. 11

Im Hinblick auf die vielfältigen Nachweispflichten, denen das Unternehmen im Datenschutz unterliegt, kann es sinnvoll sein, weitere Aspekte zur Verarbeitungstätigkeit zu dokumentieren. Diese sind nur intern zu verwenden. Zu diesen zusätzlichen Dokumentationen, die sinnvollerweise hier erfolgen, gehören z. B.

- Angaben zur Zusammenstellung der Informationspflichten (insbes. Artt. 13,14 DS-GVO)
- Verträge mit Dienstleistern (Art. 28 DS-GVO)
- Vereinbarungen zur gemeinsamen Verantwortung (Art. 26 DS-GVO)
- Eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen
- durchgeführte Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten (Art. 35 DS-GVO)

2. Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter

2.1 Prämissen

Das Verzeichnis der Verarbeitungstätigkeiten, das ein Auftragsverarbeiter zu erstellen hat (VVT-AV, Art. 30 Abs. 2 DS-GVO) dient primär dazu, eine erste Übersicht darüber zu erhalten, welche Leistungen für welchen Auftraggeber erbracht werden.

Im Gegensatz zu den heutigen Regelungen des BDSG treffen den Auftragsverarbeiter für seine Leistungen eigene Verantwortlichkeiten. So ist er zum Beispiel dafür verantwortlich, dass hinreichende Sicherheitskonzepte (siehe Art. 32 DS-GVO) oder auch die Aspekte des Privacy by Design und Default umgesetzt werden.

Die Erstellung eines VVT-AV sollte sich grundsätzlich aus Sicht des Dienstleisters und damit an seinen Standardleistungen (Produkten) orientieren. Hieraus lassen sich die „Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden“ ableiten.[6]

Bei der Bestimmung der Leistung - insbesondere bei der vertraglichen Gestaltung - sollte darauf geachtet werden, was in den Verantwortungsbereich des Auftragsverarbeiters bzw. des Auftraggebers fällt. So ist zum Beispiel die Weitergabe personenbezogener Daten an einen vom Auftragsverarbeiter eingesetzten Unterauftragnehmer im Drittland Bestandteil der vom Auftragsverarbeiter angebotenen Leistungskette. Insoweit fällt diese Weitergabe in die Sphäre des Auftragsverarbeiters und ist von ihm in seinem VVT-AV zu dokumentieren. Dagegen fällt eine vom Auftraggeber angewiesene Weitergabe seiner Daten an eine Stelle im Drittland in

6 Zur Bestimmung, was eine Standarddienstleistung ausmacht, siehe zum Beispiel den bisherigen Standard „Anforderungen an Auftragnehmer nach § 11 BDSG“ - DS-BVD-GDD-01von GDD und BvD, http://www.dsz-audit.de/wp-content/uploads/GDD-BvD-DATENSCHUTZSTANDARD-DS-BVD-GDD-01-V1-0.pdf.

die Sphäre des Auftraggebers. Die entsprechende Weisung ist zwar zu dokumentieren, nicht aber Gegenstand des VVT-AV.

Die Dokumentation von Weisungen ist nicht Gegenstand des VVT-AV. Dies betrifft die allgemeinen Weisungen sowie insbesondere die Weisungen zur Weitergabe von personenbezogenen Daten in ein Drittland. Hier ist der Auftragsverarbeiter frei, wie er eine entsprechende Dokumentation führt. Bei einer Reihe von Dienstleistern bietet sich an, hierzu in der Kommunikation mit den Auftraggebern genutzte Ticketsysteme zu nutzen. Wichtig ist allerdings dabei, dass die entsprechenden Weisungen quasi auf „Knopfdruck" aus einem solchen System herausgefiltert werden können.

Kundenspezifische Abweichungen von der angebotenen Standardleistung ergeben sich regelmäßig aus den konkreten vertraglichen Vereinbarungen, insbesondere aus dem Vertrag nach Art. 28 DS-GVO. Zur Dokumentation dieser vertraglichen Abweichungen von der Standardleistung kann auf den entsprechenden Vertrag verlinkt werden. Dabei können Anpassungen insbesondere Änderungen der Standardleistung, zum Beispiel durch Customizing, oder der vereinbarten technischen und organisatorischen Maßnahmen betreffen. Allerdings ist durch die Dokumentationsbeschränkung auf „Kategorien von Verarbeitungen" die Dokumentation der konkreten (angepassten) Leistung nicht erforderlich. Durch eine Verlinkung auf den jeweiligen Vertrag könnte jedoch die Abweichung von der Standarddienstleistung hinreichend nachvollziehbar gemacht werden.

Die im Zusammenhang mit der Weitergabe von personenbezogenen Daten an Stellen in Drittländern geforderte Dokumentation der „Garantien" ist in normalen Dienstleistungsprozessen regelmäßig entbehrlich. Dies ergibt sich daraus, dass Garantien ausschließlich in den Fällen des Art. 49 Abs. 1 und 2 DS-GVO zu dokumentieren sind. Die auf diese Regelung gestützten weitergaben dürfen allerdings nicht „wiederholt" erfolgen. Die Geschäftsprozesse eines Dienstleisters sind jedoch gerade auf eine Wiederholung angelegt. Insofern kommt diese Regelung regelmäßig nicht zur Anwendung. Eine Dokumentation anderer Garantien, wie zum Beispiel eines Angemessenheitsbeschlusses der Kommission oder durch Standardvertragsklauseln zur Drittlandsweitergabe ist nicht gefordert.

Die Ausnahmeregelungen des Art. 30 Abs. 5 DS-GVO finden auf das VVT-AV regelmäßig keine Anwendung. Dies ergibt sich insbesondere schon daraus, dass eine Befreiung von der Führung des VVT nur dann erfolgen kann, wenn die Verarbeitung nur gelegentlich erfolgt. Die Verarbeitungsprozesse eines Dienstleisters sind jedoch schon allein aus dem Geschäftszweck auf eine regelmäßige und dauerhafte Durchführung angelegt.

Der Auftragsverarbeiter bestimmt nicht die Zwecke und Mittel der (Kategorien von) Verarbeitungen. Daher steht das VVT-AV des Auftragsverarbeiters nach Art. 30 Abs. 2 DS-GVO auch nicht im Mittelpunkt des gesamten Datenschutz-Management-Systems. Es erscheint sinnvoll, dass das VVT-AV durch die dienstleistenden Fachbereiche beim Auftragsverarbeiter geführt wird oder durch die Bereiche Vertrieb/Vertragsmanagement.

Der Datenschutzbeauftragte des Auftragsverarbeiters kann im Rahmen seines Beratungsauftrags Vorschläge für Vorgaben zum VVT-AV machen und im Rahmen seines Überwachungsauftrags die Führung und Pflege dieses VVT-AV überprüfen.

2.2 Inhalte

Die Inhalte des VVT für Auftragsverarbeiter ergeben sich aus Art. 30 Abs. 2 DS-GVO:

- den Namen und die Kontaktdaten:
  - des Auftragsverarbeiters oder der Auftragsverarbeiter;
  - jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist;
  - gegebenenfalls des Vertreters des Verantwortlichen;
  - gegebenenfalls des Vertreters des Auftragsverarbeiters;
  - eines etwaigen Datenschutzbeauftragten des Auftragsverarbeiters;
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt 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 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DS-GVO.

2.3 Aufbau

Für den Aufbau des VVT wird ein 3-stufiger Aufbau empfohlen:

1. Vorblatt 1 mit den Angaben zum Auftragsverarbeiter:

- Auftragsverarbeiter: Name, ladungsfähige Adresse und Geschäftsleitung
- Vertreter des Auftragsverarbeiters: Name, ladungsfähige Adresse Geschäftsleitung (soweit erforderlich)
- Datenschutzbeauftragter[7]: Name, Telefonnummer / E-Mail-Adresse

2. Vorblatt 2 mit Angaben zu den Dienstleistungen:

- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 (z.B. Sicherheitskonzepte bzw. Verweise darauf, Zertifizierungen)
- Datenweitergabe in ein Drittland (soweit sie z. B. im Rahmen der Lieferkette in der in der Sphäre des Auftragsverarbeiters liegt)
- Kategorien der Dienstleistungen:
  - Dienstleistung 1:
    - Bezeichnung, „Kategorisierung“, Anhalt: „Leistung“ i.S.d. BvD-GDD-ADV-Standards
    - ggf. Abweichungen von der zuvor beschriebenen Datenweitergabe in ein Drittland
    - ggf. Anpassungen des Sicherheitskonzepts]
  - Dienstleistung … :
    - …

7 Hier ist nur der Datenschutzbeauftragte des Auftragsverarbeiters, der das Verzeichnis führt, aufzunehmen (analog zu Art. 30 Abs. 1 DS-GVO). Es bedarf keiner gesonderten zusätzlichen Datenerhebung bezüglich des Namens und der Kontaktdaten der Datenschutzbeauftragten der jeweiligen Auftraggeber. Diese Angaben sind auch nach Art. 28 DS-GVO nicht zur Weitergabe an den Auftragnehmer vorgesehen.

3. Hauptblatt mit den Angaben zu den Kunden:

>> **Kunde 1:**

> Verantwortlicher[8]

- Name, ladungsfähige Adresse

> Vertreter des Verantwortlichen: [

- Name, ladungsfähige Adresse (soweit erforderlich)

> Gebuchte Dienstleistungen:

> Verweise auf Vorblatt 2, ggf. Verlinkung auf Vertrag – insbesondere bei Abweichungen von der Standarddienstleistung

> …

>> **Kunde 2:**

- …

Alternativ kann sich auch die Führung des Hauptblattes in Tabellenform anbieten

VORBLATT 1	VORBLATT 2	HAUPTBLATT
Angaben zum Auftragsverarbeiter: **Auftragsverarbeiter:** • Name, ladungsfähige Adresse und Geschäftsleitung **Vertreter des Auftragsverarbeiter:** • Name, ladungsfähige Adresse und Geschäftsleitung **Datenschutzbeauftragter:** • Name, ladungsfähige Adresse und Geschäftsleitung	**Angaben zu Dienstleistungen:** **Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art 32.** • Sicherheitskonzepte bzw. Verweise darauf, Zertifizierungen **Drittlandübermittlung** • Namen **Kategorien der Dienstleistungen** >> **Dienstleistung 1** • Bezeichnung, „Kategorisierung“, Anhalt: „Leistung“ i.S.d. BvD-GDD-ADV-Standards • ggf. Anpassungen des Sicherheitskonzepts >> **Dienstleistung 2** …	**Angaben zu Kunden:** **Kunde 1:** **Verantwortlicher:** • Name, ladungsfähige Adresse **Vertreter des Verantwortlichen:** • Name, ladungsfähige Adresse **Gebuchte Dienstleistung:** **1.) …** ***Verweis auf Vorblatt 2*** **2.) …** **Kunde 2:** …

8 Verantwortlicher in diesem Sinne ist – auch in einer Leistungskette – immer der direkte Auftraggeber. Die DS-GVO sieht im Bereich der ADV eine gestufte Verantwortung vor, im Gegensatz zum BDSG, das von der „Durchgriffsverantwortung“ des Auftraggebers ausgeht. Von daher sind die Auftraggeber der „weiteren Auftragsverarbeiter“ (Unterauftragnehmer) die „Verantwortlichen“ in diesem Zusammenhang.

HAUPTBLATT

Angaben zu Kunden (alternative Darstellung einer Beziehungs-Matrix

Kunde 1:
>> Verantwortlicher:
- Name, ladungsfähige Adresse

>> Vertreter des Verantwortlichen:
- Name, ladungsfähige Adresse

Kunde 2:

...

Leistungs-beziehungen	Dienstleistung 1	Dienstleistung 2	...	Dienstleistung N
Kunde 1	X			
Kunde 2	X	X		
...				
Kunde N		X		X

3. Verzeichnis von Verarbeitungstätigkeiten für 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 oder Auftragsverarbeiter vorgenommen 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 oder Auftragsverarbeiters außerhalb der Union jedoch überhaupt habhaft werden zu können, trifft diese gem. Art. 27 Abs. 1 DS-GVO die Pflicht, schriftlich einen Vertreter zu bestellen, der innerhalb der Union niedergelassen sein muss.

Gem. Art. 27 Abs. 4 DS-GVO hat der Vertreter in der Union die Aufgabe, für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung zur Gewährleistung der Einhaltung dieser Verordnung als Anlaufstelle zu dienen.

Aus diesem Grunde hat der Vertreter in der Union das VVT vorzuhalten oder, sofern er für einen Auftragsverarbeiter benannt ist, das jeweilige VVT-AV. Hierbei handelt es sich um inhaltsgleiche Duplikate, sodass insoweit auf die obigen Ausführungen verwiesen werden kann.

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Die Inhalte dieser Praxishilfe wurden im Rahmen des GDD-Erfakreises Köln, Unterarbeitsgruppe „VVT“ erstellt.

Mit freundlicher Unterstützung des GDD-Arbeitskreises „DS-GVO Praxis“.

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 2 28 96 96 75-00
Fax: +49 2 28 96 96 75-25
www.gdd.de
info@gdd.de

Stand:
Version 1.0 (April 2017)