



Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO

Verzeichnis von Verarbeitungstätigkeiten – Auftragsverarbeiter



1. Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter

1.1 Prämissen	4
1.2 Inhalte	6
1.3 Aufbau	6

2. Verzeichnis von Verarbeitungstätigkeiten-AV für Vertreter in der EU.....

9

Verzeichnis von Verarbeitungstätigkeiten – Auftragsverarbeiter

Art. 30 DS-GVO sieht für Auftragsverarbeiter eine eigene kundenbezogene Dokumentation vor. Nach Erwägungsgrund 82 der DS-GVO soll der Auftragsverarbeiter „zum Nachweis der Einhaltung dieser Verordnung“ auch das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO führen. Die zuständige Aufsichtsbehörde kann die Vorlage verlangen, um die betreffenden Verarbeitungen hoheitlich zu kontrollieren.

Dieses Verzeichnis von Verarbeitungstätigkeiten – Auftragsverarbeiter (VVT-AV) unterscheidet sich grundlegend von der prozessbezogenen Dokumentation, die der Verantwortliche gemäß Art. 30 Abs. 1 DS-GVO zu führen hat. Daher wird ihm hier eine eigene Praxishilfe gewidmet.

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

>> Michael Gutjahr

innogy SE

>> Stefan Hardelt

Unternehmensberatung Datenschutz

>> Werner Metterhausen

VON ZUR MÜHLEN´SCHE GmbH

>> 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 Auftragsverarbeiter

1.1 Prämissen

Den Auftragsverarbeiter treffen nach der DS-GVO eine Reihe von eigenen Pflichten, für die er als Normadressat eigenverantwortlich einzustehen hat.¹

Hierzu zählt auch das Verzeichnis der Verarbeitungstätigkeiten, das er gemäß Art. 30 Abs. 2 DS-GVO zu erstellen hat (VVT-AV). Es dient primär dazu, eine erste Übersicht darüber zu erhalten, welche Leistungen für welchen Auftraggeber erbracht 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. Dabei sollte folgendes beachtet werden:

- 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 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. Soweit vorhanden bietet sich für Dienstleister 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 sind nicht Gegenstand des VVT-AV. Sie 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

¹ Zu den Anforderungen an einen Auftragsverarbeiter nach DS-GVO s. GDD-Praxishilfe DS-GVO XII – Praxishinweise für Auftragsverarbeiter.

und organisatorischen Maßnahmen betreffen. Allerdings ist durch die Dokumentationsbeschränkung auf „Kategorien von Verarbeitungen“ die Dokumentation der konkreten (angepassten) Leistung im VVT-AV nicht erforderlich. Durch eine Verlinkung auf den jeweiligen Vertrag könnte jedoch die Abweichung von der Standarddienstleistung für interne Zwecke des Dienstleisters 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 Unterabsatz 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.

Die **Einsicht in das VVT-AV** ist lediglich der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Eine Aushändigung an andere Stellen oder eine Einsicht durch sie sieht die DS-GVO nicht vor. Damit bestehen auch keine dementsprechenden Ansprüche der Auftraggeber eines Auftragsverarbeiters.

Ein Auftragsverarbeiter unterliegt für die Verarbeitungen personenbezogener Daten, die er für eigene Zwecke **als Verantwortlicher** durchführt, weiterhin der Verpflichtung zur Dokumentation dieser Prozesse gemäß Art. 30 Abs. 1 DS-GVO.

Die Erstellung, Führung und Pflege eines VVT-AV sollte durch eine **Organisationsanweisung** (z.B. Richtlinie, Policy) geregelt werden.²

² Hinweise zur Erstellung einer solchen Organisationsanweisung werden in der Praxishilfe Va gegeben. Diese Hinweise gelten sinngemäß auch für das VVT-AV.

1.2 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 Auftragsverarbeiters³;
 - > 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 Garantien⁴;
- [wenn möglich]⁵, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DS-GVO.

³ Diese Angabe dürfte in der Praxis ausgeschlossen sein, s. dazu unten unter „2. Verzeichnis von Verarbeitungstätigkeiten-AV für Vertreter in der EU“.

⁴ Diese Angabe dürfte in der Praxis regelmäßig ausgeschlossen sein, s. dazu oben unter „1.1 Prämissen“.

⁵ Die Einschränkung „wenn möglich“ sollte in der Praxis unbeachtlich sein, da der Auftragsverarbeiter zumindest im Rahmen der „Garantien“ nach Art. 28 Abs. 1 DS-GVO und seiner Nachweispflichten im Rahmen des Art. 28 Abs. 3 lit. h) DS-GVO eine entsprechende Dokumentation vorhalten muss.

1.3 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:⁶
[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 Sphäre des Auftragsverarbeiters liegt)
- Kategorien der Dienstleistungen:
 - >> Dienstleistung 1:
 - > [Bezeichnung, „Kategorisierung“, Inhalt: „Leistung“ i.S.d. BvD-GDD-ADV-Standards]

⁶ 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.

- > [ggf. Abweichungen von der zuvor beschriebenen Datenweitergabe in ein Drittland]
- > [ggf. Anpassungen des Sicherheitskonzepts]
- >> Dienstleistung ... :
 - > ...

3. Hauptblatt mit den Angaben zu den Kunden:

- Kunde 1:
 - >> Verantwortlicher⁷:
[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: <ul style="list-style-type: none"> • Auftragsverarbeiter: [Name, ladungsfähige Adresse und Geschäftsleitung] • Vertreter des Auftragsverarbeiters: [Name, ladungsfähige Adresse Geschäftsleitung] (soweit erforderlich) • Datenschutzbeauftragter⁶: [Name, Telefonnummer / E-Mail-Adresse] 	Angaben zu Dienstleistungen: <ul style="list-style-type: none"> • 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 Sphäre des Auftragsverarbeiters liegt) • Kategorien der Dienstleistungen: -> Dienstleistung 1: -> ... 	Angaben zu Kunden: <ul style="list-style-type: none"> • Kunde 1: <ul style="list-style-type: none"> >> Verantwortlicher [Name, ladungsfähige Adresse] >> Vertreter des Verantwortlichen: [Name, ladungsfähige Adresse] (soweit erforderlich) >> Gebuchte Dienstleistungen: -> ...

⁷ Verantwortlicher in diesem Sinne ist – auch in einer Leistungskette – immer der direkte Auftraggeber. Die DS-GVO sieht im Bereich der Auftragsverarbeitung eine gestufte Verantwortung vor. Von daher sind die Auftraggeber der „weiteren Auftragsverarbeiter“ (Unterauftragnehmer) die „Verantwortlichen“ in diesem Zusammenhang.

Vorblatt 1

Angaben zum Auftragsverarbeiter:

- Auftragsverarbeiter:
[Name, ladungsfähige Adresse und Geschäftsleitung]
- Vertreter des Auftragsverarbeiters:
[Name, ladungsfähige Adresse Geschäftsleitung] (soweit erforderlich)
- Datenschutzbeauftragter:⁶
[Name, Telefonnummer / E-Mail-Adresse]

Vorblatt 2

Angaben zu 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 Sphäre des Auftragsverarbeiters liegt)
- Kategorien der Dienstleistungen:
-> Dienstleistung 1:
-> ...

Hauptblatt

Angaben zu Kunden:

- Kunde 1:
 - >> Verantwortlicher
[Name, ladungsfähige Adresse]
 - >> Vertreter des Verantwortlichen:
[Name, ladungsfähige Adresse]
(soweit erforderlich)
 - >> Gebuchte Dienstleistungen:
-> ...

Hauptblatt

Angaben zu Kunden (alternative Darstellung über eine Beziehungs-Matrix)

Kunde 1:

- >> Verantwortlicher:
[Name, ladungsfähige Adresse
und Geschäftsleitung]
- >> Vertreter des Verantwortlichen:
[Name, ladungsfähige Adresse
und Geschäftsleitung]
- >> Gebuchte Dienstleistungen:

Kunde 2:

...

Leistungs- beziehung	Dienstleistung 1	Dienstleistung 2	...	Dienstleistung n
Kunde 1				
Kunde 2				
...				
Kunde n				

2. Verzeichnis von Verarbeitungstätigkeiten-AV für Vertreter in der EU

Ein Auftragsverarbeiter in einem Drittland ist regelmäßig nicht verpflichtet, einen Vertreter innerhalb der EU gemäß Art. 27 DS-GVO zu bestellen.

Zwar gilt grundsätzlich folgendes:

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.

Um des Verantwortlichen oder Auftragsverarbeiters außerhalb der Union jedoch überhaupt haftbar werden zu können, trifft diese gem. Art. 27 Abs. 1 DS-GVO grundsätzlich die Pflicht, schriftlich einen Vertreter zu bestellen, der innerhalb der Union niedergelassen sein muss.

Allerdings gilt in diesem Zusammenhang auch zu beachten:

Die Pflicht zur Bestellung eines Vertreters gem. Art. 27 Abs. 1 DS-GVO besteht nur bei Anwendbarkeit des Marktortprinzips.

Das Marktortprinzip nach Art. 3 Abs. 2 DS-GVO gilt aber nur, wenn die Datenverarbeitung im Zusammenhang damit steht, **betroffenen Personen** in der Union Waren oder Dienstleistungen anzubieten oder ihr Verhalten zu beobachten, soweit ihr Verhalten in der Union erfolgt.

Im Verhältnis Verantwortlicher (Controller) – Auftragsverarbeiter (Processor) liegen die Voraussetzungen des Art. 3 Abs. 2 DS-GVO beim Auftragsverarbeiter regelmäßig nicht vor. Sein Angebot richtet sich qua Definition der Auftragsverarbeitung stets an Verantwortliche und gerade nicht an betroffene Personen, wie es aber in Art. 3 Abs. 2 DS-GVO gefordert ist.

Die Folge ist, dass auf einen Auftragsverarbeiter im Drittland die DS-GVO keine – zumindest keine unmittelbare – Anwendung findet. Damit entfällt auch die Pflicht, einen Vertreter nach Art. 27 DS-GVO zu bestellen. Denn dieser ist nur im Falle des Art. 27 i.V.m. Art. 3 Abs. 2 zu bestellen.

Mangels Anwendbarkeit des Marktortprinzips auf den Auftragsverarbeiter im Drittland muss er auch kein VVT-AV erstellen.

Eine Schlechterstellung der Betroffenen in diesen Fällen ergibt sich nicht, da der Verantwortliche auch bei der Verarbeitung durch eine Auftragsverarbeitung im Drittland ihnen gegenüber in der vollen datenschutzrechtlichen Verantwortung und Haftung bleibt.



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

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 2 28 96 96 75-00

Fax: +49 2 28 96 96 75-25

www.gdd.de

info@gdd.de

Ansprechpartner:

Yvette Reif, LL.M.

Stand:

Version 1.0 (Januar 2020)