



Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO

Praxishinweise für Auftragsverarbeiter nach
Art. 28 DS-GVO



Vorwort	3
1. Abgrenzung Verantwortlicher und Auftragsverarbeiter	4
2. Wann bin ich Auftragsverarbeiter?	5
3. Eigene Pflichten des Auftragsverarbeiters	8
3.1 Rechtspflichten	8
3.2 Datenschutzorganisation und Datenschutzmanagementsystem	8
3.3 IT-Sicherheitsmanagementsystem	8
4. Auftraggeberübergreifende Anforderungen an den Auftragsverarbeiter	9
4.1 Inhaltliche Beschreibung der Leistung und des Herstellungsprozesses	10
4.2 In- und Outputmanagement	11
4.3 Einsatz von Unterauftragnehmern	11
4.4 IT-Sicherheitskonzept und IT-Sicherheitsmanagementsystem	11
4.5 Prozessuale Festlegungen	12
1. Auftragskontrolle	13
2. Verpflichtung der Beschäftigten auf Vertraulichkeit	13
3. Genehmigung des Einsatzes von Unterauftragnehmern	13
4. Prozessbeschreibung Auskunft, Berichtigung, Datenübertragbarkeit und Löschung	13
5. Prozessbeschreibung Datenschutzverletzung	14
6. Nachweis der Pflichten aus Art. 28 DS-GVO und Unterstützung bzw. Mitwirkung bei Kontrollen	14
7. Rückgabe / Löschung von Daten nach Vertragsende	15
5. Pflichten aus dem Auftragsverarbeitungsverhältnis	15
5.1 Vertrag zur Auftragsverarbeitung	15
5.2 Auftragsmanagement	16

Praxishinweise für Auftragsverarbeiter nach Art. 28 DS-GVO

Kern der Regelungen zur Auftragsbearbeitung ist die Regelung der Beziehung zwischen Auftraggeber und Auftragsverarbeiter. Hierbei ist sicherzustellen, dass im Zusammenwirken dieser beiden das Datenschutzniveau, das grundsätzlich der Verantwortliche (Auftraggeber) sicherzustellen hat, nicht durch die Verlagerung auf den Dienstleister unterschritten wird. Daher muss sich auch der Auftragsverarbeiter auf seiner Seite der Schnittstelle auf die diesbezüglichen Anforderungen einstellen.

Mit Einführung der DS-GVO ist der Auftragsverarbeiter neben dem Verantwortlichen als Normadressat getreten. Dies gilt sowohl für die Kernnorm der Auftragsverarbeitung gem. Art. 28 DS-GVO, als auch viele weitere Normen, in denen die Verantwortlichkeit des Auftragsverarbeiters ausdrücklich genannt wird. Verschärft wird diese Situation durch die Haftungs- und Bußgeldregelungen (Artt. 82 und 83 DS-GVO) sowie ein direktes Klagerecht der betroffenen Personen gegen den Auftragsverarbeiter.

Dies alles macht es unumgänglich, dass sich der Auftragsverarbeiter

- mit den ihm aus der DS-GVO obliegenden Pflichten auseinandersetzt und
- sich bereits bei der Konzeption und Planung seiner Dienstleistung sorgfältig auf Datenschutzaspekte, denen seine potenziellen Auftraggeber ausgesetzt sein können, einstellt und datenschutzkonforme Lösungen implementiert.

Eine vorausschauende Prozessgestaltung ist im Hinblick auf die eigene Entlastung im Haftungsfall zwingend erforderlich.

Neben den hier gegebenen Hinweisen sollten sich gerade auch KMU als Auftragsverarbeiter zur eigenen Entlastung mit der genehmigten Verhaltensregel „Anforderungen an Auftragsverarbeiter nach Art. 28 DS-GVO“ - „TRUSTED DATA PROCESSOR“ beschäftigen. Hier werden weitere Konkretisierungen für zentrale Datenschutzprozesse bei Auftragsverarbeitern gegeben.

Diese Praxishinweise der GDD möchten Hilfestellungen für **Auftragsverarbeiter** geben, wie die gesetzlichen Vorgaben insbesondere an der Schnittstelle zu seinen Auftraggebern umgesetzt werden können.

Weitergehende grundsätzliche Hinweise zur Auftragsverarbeitung sowie einen Mustervertrag finden Sie in der **GDD-Praxishilfe DS-GVO – Mustervertrag zur Auftragsverarbeitung**.

1. Abgrenzung Verantwortlicher und Auftragsverarbeiter

Die Begriffe „Verantwortlicher“ und „Auftragsverarbeiter“ spielen bei der Anwendung der DS-GVO eine entscheidende Rolle, da sie bestimmen, wer in welchem Umfang für die Einhaltung der verschiedenen Datenschutzvorschriften verantwortlich ist.¹

„**Verantwortlicher**“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Abs. 7 DS-GVO). „**Auftragsverarbeiter**“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Abs. 8 DS-GVO).

Entsprechend der Leitlinien 07/2020² des Europäischen Datenschutzausschusses (EDSA) sind für die Abgrenzung folgende Kriterien maßgebend:

Zumindest in Bezug auf den Zweck der Verarbeitung und die wesentlichen Mittel, wie Art und Dauer der Verarbeitung, Kategorien von betroffenen Personen und Empfängern muss der Auftragsverarbeiter die Weisungen des Verantwortlichen umsetzen. Bei den praktischen Aspekten der Umsetzung, wie die Wahl einer bestimmten Hard- oder Software oder die installierten Sicherheitsmaßnahmen, kann der Auftragsverarbeiter – soweit nicht anders vereinbart - entscheiden.



Nach Art. 28 Abs. 10 DS-GVO wird der Auftragsverarbeiter selbst Verantwortlicher, wenn er über die Weisungen des Verantwortlichen hinausgeht und eigene Zwecke und Mittel der Verarbeitung festlegt. Er kann dann als Verantwortlicher, insbes. für eine Verarbeitung ohne Rechtsgrundlage, sanktioniert werden!

Verantwortlicher

Alleinige oder gemeinsame Entscheidung über **Zwecke und** (zumindest „wesentliche“) **Mittel**

- Definition „Zweck“:
„ein erwartetes Ergebnis, an dem sich ihre geplanten Maßnahmen ausrichten“
- Definition „Mittel“:
„auf welche Weise dieses Ziel erreicht werden soll“

Auftragsverarbeiter

- „Entscheidungen über den Zweck der Verarbeitung sind eindeutig stets Sache des Verantwortlichen“
- Der Auftragsverarbeiter kann entscheiden über „nicht wesentliche Mittel“, wie die Wahl einer bestimmten Hard- oder Software oder die detaillierten Sicherheitsmaßnahmen

¹ Zur Abgrenzung s.a. GDD Praxishilfe DS-GVO - Mustervertrag zur Auftragsverarbeitung, S. 4 ff und Hilfen in GDD-Praxishilfe DS-GVO - Die gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO (Joint Controllership), Kap. 9, S. 23 ff.

² EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO, Version 2.0, Juli 2021.

Gem. Art. 4 Abs. 10 DS-GVO ist die Auftragsverarbeitung dergestalt privilegiert, dass der Auftragsverarbeiter kein Dritter ist. Eine Beschränkung der Privilegierung auf den EU-/EWR-Raum erfolgt nicht. Auftragsverarbeiter im Drittland sind damit ebenfalls keine „Dritten“ für den Verantwortlichen.

2. Wann bin ich Auftragsverarbeiter?

Auftragsverarbeiter verarbeiten personenbezogene Daten im Auftrag des Verantwortlichen und auf Basis seiner Weisungen. Da die Leistungen eines Dienstleisters sehr vielschichtig sind, muss im Rahmen einer **Einzelfallprüfung** untersucht werden, ob eine Verarbeitung personenbezogener Daten im Auftrag vorliegt.

Es bestehen jedoch **Kriterien**, die bei der Prüfung zur Einordnung als Verantwortlicher oder Auftragsverarbeiter Unterstützung leisten können. So kann eine Stelle, die über die **Zwecke der Verarbeitung** personenbezogener Daten entscheidet, kein Auftragsverarbeiter sein. Bei der Beurteilung dieses Kriteriums ist zu untersuchen,

- >> welchen Umfang der Handlungsspielraum des Dienstleisters bei der Auftragsverarbeitung hat,
- >> wie der Dienstleister durch den Auftraggeber überwacht wird,
- >> die Expertise des Dienstleisters bei der Auftragsverarbeitung,
- >> die Transparenz des Dienstleisters gegenüber dem Betroffenen.

Gleiches gilt für eine Stelle, die über die **wesentlichen Mittel** einer Verarbeitung entscheidet. Eine Entscheidung über „wesentliche Mittel“ einer Datenverarbeitung liegt in der Regel bei folgenden Punkten vor:

- >> welche Daten verarbeitet werden,
- >> wie lange sie verarbeitet werden,
- >> wer Zugang zu ihnen hat.

Die – alleinige – Entscheidung des Auftragsverarbeiters über **technisch-organisatorische Mittel** ist kein Ausschlussgrund für eine Auftragsverarbeitung.

Stellt sich die Bewertung, ob es sich bei der zu betrachtenden **Dienstleistung** um eine **Auftragsverarbeitung** oder um eine **sonstige Outsourcing-Lösung** handelt als schwierig dar, so können verschiedene Indizien³ für eine klarere Unterscheidung herangezogen werden:

- >> Eine bestehende **Weisungsabhängigkeit** zwischen dem Auftraggeber und dem Dienstleister spricht für das Vorliegen einer Auftragsverarbeitung;
- >> Stellt sich die relevante Datenverarbeitung nicht als die **Hauptleistung** des Dienstleisters, sondern vielmehr als eine **reflexartige Nebenerscheinung** für die Erbringung einer davon unabhängigen Leistung dar, kann dies als **Indiz** gegen eine Auftragsverarbeitung und für eine **Übermittlung** berücksichtigt werden;
- >> Hat der **Auftragnehmer** ein **eigenes wirtschaftliches Interesse** an den Daten oder dem Ergebnis der Datenverarbeitung kann dies als weiteres Indiz für eine **Übermittlung** betrachtet werden;
- >> Ein **eigenes rechtliches Verhältnis** zwischen Auftragnehmer und Betroffenen kann ebenfalls ein **Anhaltspunkt** dafür sein, dass keine Auftragsverarbeitung, sondern eine Übermittlung im Vordergrund steht;
- >> Kommt eine **Haftung des Auftragnehmers** für die **Richtigkeit** oder **Rechtmäßigkeit der Datenverarbeitung** in Frage, spricht auch dies eher für das Vorliegen einer Übermittlung.

³ Franck, Studienheft Nr. 385 - Datenschutzrecht, 2. Aufl. 2018, Bad Sooden, S. 41.

Ein möglicher Ablauf zur Einordnung des Dienstleisters als Verantwortlicher oder Auftragsverarbeiter ist dem nachfolgenden Schaubild zu entnehmen:

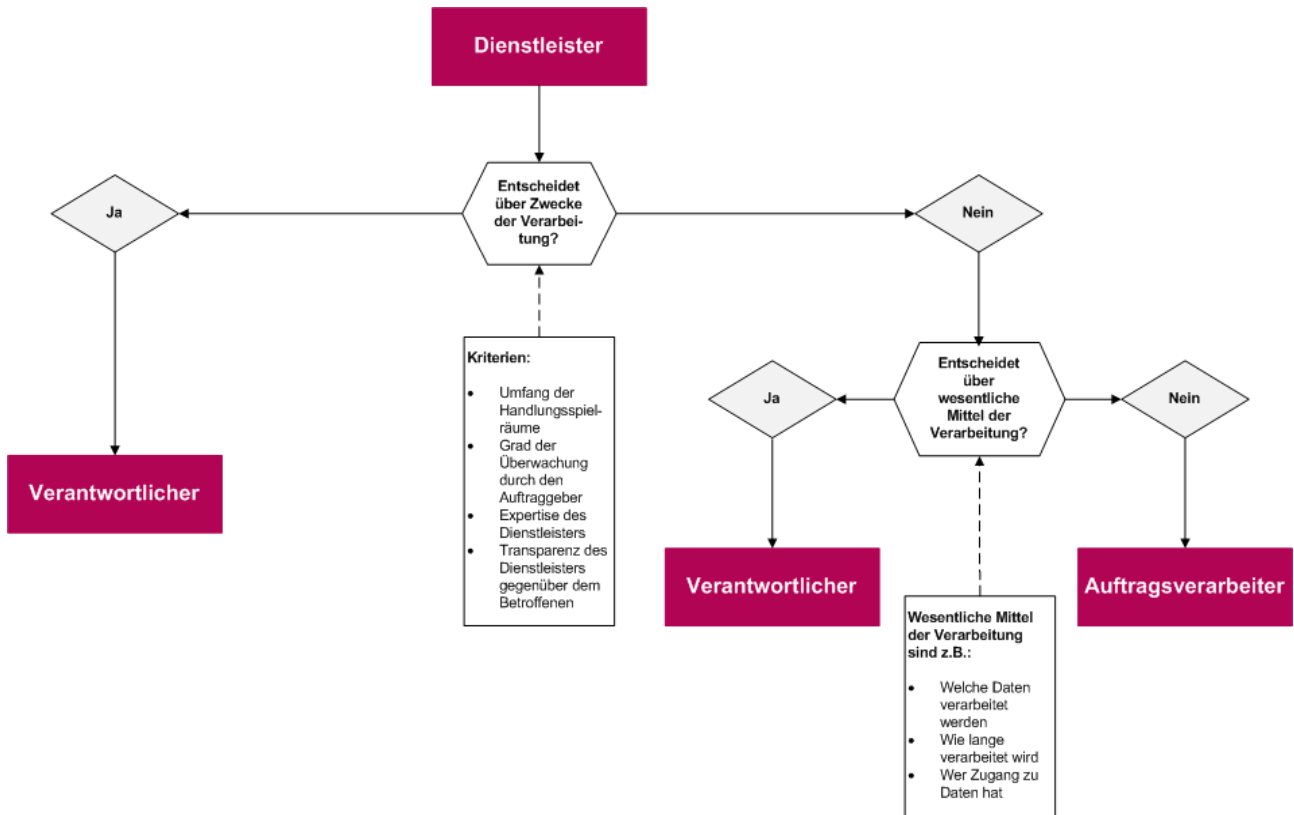


Abbildung 1: Einordnung Dienstleister

Die Aufsichtsbehörden haben verschiedene Orientierungshilfen mit Beispielen für die Verarbeitung personenbezogener Daten als Auftragsverarbeitung bzw. als keine Auftragsverarbeitung veröffentlicht⁴.



⁴ z.B. EDSA, a.a.O., DSK Kurzpapier Nr. 13, BayLDA Auftragsverarbeitung – Orientierungshilfe Version 2.0, April 2019.

Auftragsverarbeitung

- Werbeadressverarbeitung in einem Lettershop
- Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten
- Outsourcing im Rahmen von Cloud-Computing, ohne dass ein inhaltlicher Datenzugriff des Cloud-Betreibers erforderlich ist
- DV-technische Arbeiten, z.B. für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren
- Verarbeitung von Kundendaten durch ein Callcenter
- Auslagerung der E-Mail-Verwaltung oder von sonstigen Datendiensten zu Webseiten (z.B. Betreuung von Kontaktformularen oder Nutzeranfragen)
- Datenträgerentsorgung durch Dienstleister
- Prüfung oder Wartung (z.B. Fernwartung, externer Support) soweit bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann

Keine Auftragsverarbeitung

Externe Inanspruchnahme von Aufgaben/Funktionen wie

- Berufsheimnisträger (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer)
- Inkassobüros mit Forderungsübertragung
- Bankinstitute für den Geldtransfer
- Postdienste für den Brieftransport
- Mitarbeiterrekrutierung
- Vertragskundenbetreuung
- Finanzberatung
- Unternehmensberatung
- Sachverständigen- bzw. Gutachtenbeauftragung an/durch Dritte mit eigenverantwortlicher Wahrnehmung
- Bewachungsdienste
- Reinigungsdienstleistungen
- Handwerkereinsätze im Unternehmen für Reparaturen und Wartung



Die Einstufung als Auftragsverarbeiter oder Verantwortlicher muss mit Blick auf konkrete Datensätze oder Vorgänge geprüft werden.



3. Eigene Pflichten des Auftragsverarbeiters

3.1 Rechtspflichten

Mit Anwendung der DS-GVO werden dem Auftragsverarbeiter in zahlreichen Normen eigene **Rechtspflichten** auferlegt, die er als **Normadressat** zu erfüllen hat.

Dazu gehören u.a.

- >> Das Ergreifen technischer und organisatorischer Maßnahmen der Datensicherheit (Art 32 DS-GVO)
- >> Die Bestellung sowie ordnungsgemäße und frühzeitige Einbindung eines Datenschutzbeauftragten, sofern erforderlich (Artt. 37 und 38 DS-GVO)
- >> Die Führung eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 Abs. 2)
- >> Die Zusammenarbeit mit der Aufsichtsbehörde (Art. 31 DS-GVO)
- >> Die Einhaltung der Bedingungen für die Verarbeitung personenbezogener Daten in Drittländern (Art. 44 ff. DS-GVO)
- >> die Einhaltung sämtlicher sich aus dem Auftragsverhältnis ergebender Pflichten (Artt. 28, 29, 33 und 36 DS-GVO)

Art. 82 Abs. 2 Satz 2 beschränkt die gesamtschuldnerische Haftung des Auftraggebers, wenn der Auftraggeber den ihm auferlegten Pflichten nachgekommen ist.

3.2 Datenschutzorganisation und Datenschutzmanagementsystem

Ein Auftragsverarbeiter agiert datenschutzrechtlich gesehen in einer Doppelrolle: einmal als Verantwortlicher (für die Datenverarbeitungsprozesse seiner eigenen Organisation) und im Hinblick auf die Datenverarbeitung für seine Auftraggeber als Auftragsverarbeiter. Die diesbezüglichen Verantwortlichkeiten sind nicht deckungsgleich und müs-

sen daher gesondert betrachtet bzw. organisiert werden.

Daher sind auch im Hinblick auf die eigenen datenschutzrechtlichen Verantwortlichkeiten des Auftragsverarbeiters die für die Einhaltung der datenschutzrechtlichen Anforderungen erforderlichen Prozesse, Strukturen und Regelwerke zu schaffen (Datenschutzorganisation) und ein System zur kontinuierlichen Verbesserung der Datenschutz-Situation zu implementieren (Datenschutz-Managementsystem).

Hilfestellung hierzu geben insbesondere die GDD-Praxishilfen „Accountability“, „Verantwortlichkeiten und Aufgaben nach der DS-GVO“ und „Die Datenschutzrichtlinie“.

3.3 IT-Sicherheitsmanagementsystem

Ein funktionierendes und dokumentiertes IT-Sicherheitsmanagementsystem nach dem **Stand der Technik** gemäß Art. 32 DS-GVO ist integraler Bestandteil eines wirksamen Datenschutzes. Neben dem Nachweis der Wirksamkeit eines solchen Managementsystems sind auch die Schnittstellen zwischen Datenschutz-Managementsystem und dem IT-Sicherheitsmanagement sowie eine redundanzfreie Regelungspyramide von hoher Wichtigkeit. Prozesse zur **kontinuierlichen Verbesserung** und einer **Wirksamkeitsprüfung** müssen vorhanden sein.

Der Nachweis eines etablierten IT-Sicherheitsmanagementsystems ist durch die Einhaltung genehmigter Verhaltensregeln (Art. 40 DS-GVO) oder ein Zertifikat möglich (Art. 42 DS-GVO), Art. 32 Abs. 3 DS-GVO.

Hinweis:

Eine Zertifizierung nach BSI-Grundschutz bzw. ISO 27001 entspricht nicht den Anforderungen des Art. 42 DS-GVO.

4. Auftraggeberübergreifende Anforderungen an den Auftragsverarbeiter

Es spricht daher vieles dafür, dass ein Auftragsverarbeiter sich vor dem Abschluss konkreter Auftragsverarbeitungsverträge proaktiv mit den rechtlichen, organisatorischen und prozessualen Datenschutzfragestellungen seiner angebotenen Leistungen beschäftigt. Schließlich ist er im Sinne von Art. 28 DS-GVO insbesondere verpflichtet⁵:

- >> sein Dienstleistungsangebot, seine internen Prozesse sowie die technischen und organisatorischen Maßnahmen (TOM) an die Anforderungen der DS-GVO anzupassen,
- >> ein entsprechendes Datensicherheitskonzept und ein IT-Sicherheitsmanagement zu etablieren,
- >> seine Infrastruktur und TOMs permanent zu überprüfen, um den „Stand der Technik“ zu gewährleisten,
- >> auch die auftragsbezogenen Verarbeitungen in einem Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren (Art. 30 Abs. 2) und
- >> seine Verträge mit seinen Auftraggebern entsprechend den Anforderungen der DS-GVO zu gestalten.

Darüber hinaus darf ein Auftraggeber Auftragsverarbeitungsverträge nur mit solchen Auftragsverarbeitern schließen, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt.⁶ Solche Garantien

können durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder genehmigte Zertifizierungsverfahren gemäß Art. 42 DS-GVO nachgewiesen werden.⁷ Während es im Moment in Deutschland noch keine Zertifizierungen in diesem Sinne gibt, bietet die Einhaltung der Verhaltensregel „Anforderungen an Auftragsverarbeiter nach Art. 28 DS-GVO“ - „TRUSTED DATA PROCESSOR“⁸ einen solchen Nachweis im Sinne des Art. 40 DS-GVO.

Weiter sollte ein Auftragsverarbeiter frühzeitig klären, welche Unterstützungsleistungen ggü. potenziellen Auftraggebern kommerziell mit der Vergütung für die Hauptleistung umfasst sind und bei welchen unter Umständen weitere Kosten entstehen können.

Dadurch wird das Risiko von Missverständnissen und Zeitverlusten bei einer konkreten Anfrage bzw. einem konkreten Angebot reduziert und der Auftragsverarbeiter kann „seine Standards“ transparent und strukturiert platzieren und idealerweise etablieren.

Mit Inkrafttreten der DS-GVO ist der in früheren Datenschutzgesetzen enthaltene Ordnungsrahmen für die Darstellung des Datenschutzniveaus bei den technischen und organisatorischen Maßnahmen entfallen und es hat sich bisher auch kein neues Ordnungsschema etabliert. Eine Hilfestellung insbesondere für kleine und mittlere Unternehmen, die als Auftragsverarbeiter im Sinne der DS-GVO arbeiten oder arbeiten möchten, bietet das Datenschutz-Reifegradmodell zur Abbildung von technisch-organisatorischen Maßnahmen bei der Auftragsverarbeitung der Bitkom⁹. In unterschiedlichen Themengebieten lassen sich die eigenen Fähigkeiten einordnen, Defizite erkennen sowie zielgerichtete Weiterentwicklungen ableiten.

⁵ Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V. (Hg.): Die DS-GVO – Hinweise für kleiner und mittlere Unternehmen, 2. Auflage, 2022, S. 71f.

⁶ Art. 28 Abs. 1 DS-GVO.

⁷ Art. 28 Abs. 5 DS-GVO.

⁸ VEREIN ZUR FÖRDERUNG VON VERHALTENSREGELN (VFV), Verhaltensregel „Anforderungen an Auftragsverarbeiter nach Art. 28 DS-GVO“ - „TRUSTED DATA PROCESSOR“, Version 1.0 v. 09.06.2022, 1. Auflage 2022. Die Verhaltensregel ist frei verfügbar und kann auch ohne Beitritt als Orientierung genutzt werden, dann allerdings ohne die erleichternden Wirkungen i.S.d. Art. 28 Abs. 5, 40 DS-GVO.

⁹ Leitfaden Datenschutz-Reifegradmodell - Reifegradmodell zur Abbildung von technisch-organisatorischen Maßnahmen bei der Auftragsverarbeitung, Betaversion Juli 2022.

VfV: Verhaltensregel „Anforderungen an Auftragsverarbeiter nach Art. 28 DS-GVO“ - „TRUSTED DATA PROCESSOR“:

Der Verein zur Förderung von Verhaltensregeln (VfV) e.V. verfolgt gemäß seiner satzungsmäßigen Aufgaben insbesondere das Ziel, Verhaltensregeln zu erstellen, anzupassen und einzureichen. Basierend auf der Erfahrung seiner Mitglieder GDD und BvD hat er die Verhaltensregel im Sinne des Art. 40 DS-GVO „Anforderungen an Auftragsverarbeiter nach Art. 28 DS-GVO“ - „TRUSTED DATA PROCESSOR“ entwickelt und beim LDI Baden-Württemberg genehmigen lassen.

Danach müssen Auftragsverarbeiter, die sich auf die Einhaltung dieser Verhaltensregel verpflichten, die dort beschriebenen Anforderungen umsetzen, die der Standardisierung und Transparenz der Prozesse von der Auftragsvergabe bis zur Einhaltung der Pflichten nach Art. 28 DS-GVO dienen. Ihre Einhaltung müssen Sie darüber hinaus gegenüber der DSZ als Kontrollstelle¹⁰ nachweisen. Auftraggeber dürfen darauf vertrauen, dass die verpflichteten Auftragsverarbeiter, wie in dieser Verhaltensregel beschrieben, agieren. Für die von der Selbstverpflichtung umfassten Anforderungen aus Art. 28 DS-GVO wirkt die Selbstverpflichtung als Faktor im Rahmen der Garantien i.S.d. Art. 28 Abs. 1 DS-GVO. Die Vorgaben der Verhaltensregel sollen insbesondere KMU in ihrer Rolle als Auftragsverarbeiter helfen, die erforderlichen Prozesse zu etablieren und ihren Auftraggebern in geeigneter, vereinfachter Weise nachzuweisen.

4.1 Inhaltliche Beschreibung der Leistung und des Herstellungsprozesses

Die Leistungsbeschreibung dient der Definition des zu betrachtenden Gegenstandes einer Auftragsverarbeitung im Sinne des Art. 28 DS-GVO, der Definition anderer Dienstleistungen des Auftragsverarbeiters und der Abgrenzung zur eigengenutzten internen (IT-)Infrastruktur.

Die Leistungsbeschreibung ist die verbindliche Grundlage für eine spätere Gestaltung einer konkreten Vertragsbeziehung zwischen Verantwortlichem und Auftragsverarbeiter und sorgt für die erforderliche **Transparenz der Datenverarbeitung**.

Es bietet sich an, dass der Anbieter einer Dienstleistung (Auftragsverarbeiter) seine Produkte / Leistungen im Hinblick auf den Gegenstand, den Umfang, die Art und den Zweck der Datenverarbeitung darstellt und die gewählten angemessener Datenschutz- und IT-Sicherheitsmaßnahmen beschreibt. Es bietet sich u.U. an, vereinfachte Darstellungen für die Angebotsphase und konkrete Musterklauseln in der Vertragsphase zu nutzen.

Die „Herstellung“ der Dienstleistung, sprich deren **operative Durchführung**, muss detailliert beschrieben sein. Die Dokumentation muss hinreichend vollständig, einheitlich und in sich schlüssig für Prozesse einer Dienstleistung vorgelegt werden können.

Als Inhalte bieten sich an:

- >> Flussdiagramme und Schnittstellen
- >> Eingesetzte Systeme, Hard- und Software
- >> Verantwortlichkeiten für den Datenumgang
- >> Eingesetzte weitere (Unter-)Auftragsverarbeiter
- >> Qualitätssicherungsprozesse
- >> Maßnahmen hinsichtlich Privacy by Design and by Default

¹⁰ DSZ Datenschutz Zertifizierungsgesellschaft mbH, <https://www.dsz-audit.de/>

4.2 In- und Outputmanagement

Sofern die Leistungserbringung Datenweitergaben vom Verantwortlichen zum Auftragsverarbeiter in großem Umfang oder/und in hoher Regelmäßigkeit erfordert, sollte der Auftragsverarbeiter seine inhaltliche Leistungsbeschreibung um eine allgemeine Beschreibung der Abläufe der technischen Weitergabe und die hierzu vorgesehenen Schutzmaßnahmen ergänzen.

Ebenso sind die Datenweitergaben vom Auftragsverarbeiter zum Verantwortlichen als Teil der Leistungserbringung zu beschreiben. Eine Weitergabe von Daten vom Auftragsverarbeiter zum Verantwortlichen oder die Weitergabe an eine dritte Stelle muss sicher hinsichtlich **Vertraulichkeit** und **Integrität** sein und darf ausschließlich von hierfür **autorisierten Personen** durchgeführt werden.

Hierzu müssen Beschreibungen über

- >> Abläufe der Datenübertragung,
 - >> ein Berechtigungskonzept,
 - >> die Protokollierung der Datenweitergabe,
 - >> die Möglichkeiten eines Datenexports für die eingesetzten IT-Systeme
- vorliegen.

Beim Einsatz weiterer Dienstleister sowie externer Stellen sind auch hier die In- und Output-Prozesse mit den entsprechenden Schutzmaßnahmen zu dokumentieren. Bei Verwendung externer Datenquellen ist zudem die Rechtsgrundlage für die Datenverarbeitung zu dokumentieren.

4.3 Einsatz von Unterauftragnehmern

Erfordert die Leistungserbringung eines Auftragsverarbeiters den Einsatz von Unterauftragnehmern, sind diese mit ihren jeweiligen Leistungen und den Schutzmaßnahmen ebenfalls detailliert zu dokumentieren, um einem Auftraggeber die erforderlichen Informationen vor einem Vertragsabschluss

geben zu können. Der Auftragsverarbeiter sollte intern klare Vorgaben haben, welche Standardverträge bei der Einbindung von Unterauftragnehmern aus der EU / dem EWR und in Drittstaaten zur Anwendung kommen und welche Kontrollprozesse des Auftragsverarbeiters ggü. Unterauftragnehmern existieren (inkl. Dokumentation).

Es besteht grundsätzlich eine Informationspflicht des Auftragsverarbeiters und Zustimmungserfordernis des Auftraggebers. Entsprechende Prozesse sind zu etablieren. Gem. Art. 28 Abs. 4 DS-GVO hat der Auftragsverarbeiter sicherzustellen, dass den Subunternehmen mittels Vereinbarung dieselben Datenschutzpflichten auferlegt werden, wie im Vertrag zwischen Auftraggeber und Auftragsverarbeiter. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jedes anderen Auftragsverarbeiters.

Im Datenschutz-Managementsystem des Auftragsverarbeiters sollten entsprechende Regelungen und Prozesse zur regelmäßigen Kontrolle der Unterauftragnehmer, die für die Leistungserbringung wesentlich sind und/oder Zugriff auf Auftragsdaten erhalten, definiert werden.

Konkrete Vorgaben für die Einbeziehung von Unterauftragnehmern macht zum Beispiel die Verhaltensregel „Trusted Data Processor“.¹¹

4.4 IT-Sicherheitskonzept und IT-Sicherheitsmanagementsystem

Das IT-Sicherheitskonzept soll den Schutz der Auftragsdaten **beschreiben**. Dazu müssen alle **Räume**, **Infrastrukturen** und **IT-Geräte** betrachtet werden, die die Sicherheit der personenbezogenen Daten im Rahmen der Auftragsverarbeitung beeinflussen können.

Netzwerke sind zu betrachten, soweit durch sie Auftragsdaten fließen oder **Geräte**, die Auftragsdaten speichern oder verarbeiten, an diesem Netzwerk

¹¹ DVfV, „Trusted Data Processor“, Kapitel 4.1, 4.2, 4.3.

angeschlossen sind. **Weitere Auftragsverarbeiter** (Unterauftragnehmer) sind in die Betrachtung einzubeziehen, soweit sie

- >> Zugriff auf Auftragsdaten erlangen können (z.B. Hard- und Softwarewartung, als Administratoren),
- >> für die Leistungserbringung relevant sind (z.B. Rechenzentren, Cloud-Anbieter, Druckereien, Logistikunternehmen).

Das vom Auftragsverarbeiter im Kontext der angebotenen Leistung(en) zu erstellende IT-Sicherheitskonzept hat die Vorgaben zur Risikoabschätzung des Art. 32 Abs. 1 DS-GVO zu berücksichtigen und sollte einem etablierten Standard (z.B. BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“) folgen.

Ist die Art der Auftragsdaten durch den Auftragsverarbeiter nicht erkennbar (z.B. beim Hosting), beschreibt das IT-Sicherheitskonzept das angebotene Schutzniveau. Die Beschreibung muss hinsichtlich ihrer Konkretheit und Detaillierung einen Verantwortlichen in die Lage versetzen können, zu beurteilen, ob das **angebotene Schutzniveau** für seinen konkreten Schutzbedarf angemessen ist.

Die Gewährleistung der Trennung von Daten ermöglicht, dass verschiedene Verantwortliche datenschutzkonforme Datenverarbeitungen von demselben Auftragsverarbeiter durchführen (lassen) können. Die Trennung kann auch ganz oder teilweise auf logischer Ebene stattfinden. Ein **Berechtigungskonzept** sorgt dafür, dass Daten von verschiedenen Auftraggebern getrennt verarbeitet werden können.

Ein funktionierendes und dokumentiertes IT-Sicherheitsmanagementsystem nach dem **Stand der Technik** gemäß Art. 32 DS-GVO ist integraler Bestandteil eines wirksamen Datenschutzes. Neben dem Nachweis der Wirksamkeit eines solchen Managementsystems sind auch die Schnittstellen zwischen Datenschutz-Managementsystem und dem IT-Sicherheitsmanagement sowie eine redundanzfreie Regelungspyramide von hoher Wichtigkeit. Prozesse zur **kontinuierlichen Verbesserung** und einer **Wirksamkeitsprüfung** müssen vorhanden sein.

4.5 Prozessuale Festlegungen

Die im Art. 28 DS-GVO vertraglich zu regelnden Sachverhalte erfordern vom Auftragsverarbeiter die Implementierung entsprechender Prozesse zur

1. Dokumentation und Prüfung von Weisungen des Verantwortlichen und Sicherstellung ihrer Umsetzung (**Auftragskontrolle**)
2. Verpflichtung der Beschäftigten auf Vertraulichkeit
3. Genehmigung des Einsatzes von Unterauftragnehmern und damit verbundene Pflichten
4. Unterstützung des Auftraggebers bei der Wahrnehmung von Betroffenenrechten
5. Unterstützung des Auftraggebers bei seinen Pflichten gem. Artt. 32 – 36 DS-GVO
6. Bereitstellung aller Informationen zum Nachweis der Pflichten und Unterstützung von bzw. Mitwirkung bei der Ausübung von Kontrollen des Auftraggebers
7. zur Rückgabe von Daten und Datenträgern bzw. die Löschung von Daten nach Beendigung des Vertragsverhältnisses

Auch wenn die Ausprägung dieser Prozesse je nach Auftrag variieren kann, empfiehlt es sich auf Seiten des Auftragsverarbeiters Standards zu definieren, die die grundsätzliche Erfüllung der Anforderungen sicherstellen und im Unternehmen etablieren. Spezifische auftragsbezogene Ausprägungen sind dann im Rahmen des Auftragsmanagements (s. Punkt 5.2) zu dokumentieren und in der Praxis zu etablieren.

Darüber hinaus hat der Auftragsverarbeiter sicherzustellen, dass er ein Verzeichnis der Verarbeitungen gem. Art. 30 Abs. 2 DS-GVO (VVT-AV) mit einer kundenbezogenen Dokumentation der „durchgeführten Tätigkeiten“ führt. Zum Aufbau des VVT-AV siehe GDD-Praxishilfe DS-GVO „Verzeichnis von Verarbeitungstätigkeiten Auftragsverarbeitung“.

1. Auftragskontrolle

Die Auftragskontrolle gewährleistet, dass personenbezogene Daten nur **weisungsgebunden** verarbeitet werden (vgl. Art. 29 DS-GVO). Der diesbezügliche Prozess muss bis zur untersten Ebene der Leistungserbringung Gültigkeit besitzen. Elementare Bestandteile der Auftragskontrolle sind:

- >> Regelung der Form der Weisung (schriftlich oder in Textform)
- >> Dokumentation und Archivierung von Weisungen
- >> Weisungsbefugte Personen und befugte Empfänger sind definiert
- >> Weisungen werden auf Datenschutzkonformität geprüft (Change Management)
- >> Sicherstellung der Umsetzung

Konkrete Vorgaben für die Durchführung einer solchen „Eigenkontrolle“ macht zum Beispiel die Verhaltensregel „Trusted Data Processor“.¹²

2. Verpflichtung der Beschäftigten auf Vertraulichkeit

Der Auftragsverarbeiter gewährleistet, dass sich alle Personen, die von ihm mit der Bearbeitung und der Erfüllung von Auftragsverarbeitungen betraut werden können, mit einer entsprechenden Verpflichtungserklärung auf Vertraulichkeit verpflichtet haben, bevor die Beschäftigten mit der Bearbeitung oder Erfüllung konkreter Auftragsverarbeitungsverträge betraut werden.

Konkrete Hinweise für die Durchführung einer solchen Verpflichtung macht zum Beispiel die Verhaltensregel „Trusted Data Processor“.¹³

3. Genehmigung des Einsatzes von Unterauftragnehmern

Art. 28 Abs. 2 DS-GVO erfordert die gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen und verpflichtet den Auftragsverarbeiter

über Änderungen zu informieren. Es sind daher entsprechende Prozesse zu etablieren, die eine

- >> Information des Verantwortlichen bei Änderungen von Unterauftragnehmern
 - >> Dokumentation von Genehmigungen von Verantwortlichen
 - >> Dokumentation von Widersprüchen von Verantwortlichen
- sicherstellen.

Da dem Auftragsverarbeiter gem. Art. 28 Abs. 4 DS-GVO die Pflicht trifft, den Unterauftragnehmern mittels Vereinbarungen „dieselben Pflichten“ aufzuerlegen, empfiehlt es sich Regeln für die Unterbeauftragung festzulegen und diese im Auftragsmanagementsystem zu verankern.

Konkrete Vorgaben zur Genehmigung des Einsatzes von Unterauftragnehmern macht zum Beispiel die Verhaltensregel „Trusted Data Processor“.¹⁴

4. Prozessbeschreibung Auskunft, Berichtigung, Datenübertragbarkeit und Löschung

Die Wahrung und Bearbeitung von geltend gemachten Betroffenenrechten gem. Artt. 15 ff. obliegt dem Verantwortlichen und nicht dem Auftragsverarbeiter. Der Auftragsverarbeiter hat aber in jedem Fall grundsätzliche Verantwortlichkeiten und Prozesse für **Unterstützungsleistungen** des für die Verarbeitung Verantwortlichen zu etablieren. Der Auftragsverarbeiter sollte u.a. vorsehen, dass

- >> **Rollen, Tätigkeiten und Verantwortlichkeiten** im Hinblick auf den Auskunftsprozess auf Seiten des Auftragsverarbeiters und die Schnittstelle zum Verantwortlichen **umfassend beschrieben** sind,
- >> auftragsbezogene Begehren von Betroffenen geordnet entgegengenommen und unverzüglich an den zuständigen Verantwortlichen **weitergeleitet** werden, es sei denn der Auftragsverarbeiter hat sich vertraglich zur Beauskunftung für den Verantwortlichen verpflichtet,

¹² VfV, „Trusted Data Processor“, Kapitel 4.7.

¹³ VfV, „Trusted Data Processor“, Kapitel 4.6.

¹⁴ VfV, „Trusted Data Processor“, Kapitel 4.2.

- >> alle berechtigten Begehren **zeitnah** und **vollständig** erfüllt werden können (technische Umsetzung). Dabei sind **Rechte Dritter** zu wahren, so dürfen z.B. im Rahmen eines Auskunftsbeglehrens keine Daten anderer Personen, Mitarbeiter oder Verantwortlicher mitbeauskunftet werden,
- >> eine **Qualitätskontrolle** etabliert ist,
- >> eingesetzte **Unterauftragnehmer** über eingehende **Lösch- oder Berichtigungsanfragen** von Betroffenen informiert und die Löschung bzw. Berichtigung der personenbezogenen Daten umgesetzt wird.

Konkrete Vorgaben zur Gestaltung der Prozesse zur Sicherstellung der Betroffenenrechte macht zum Beispiel die Verhaltensregel „Trusted Data Processor“.¹⁵

5. Prozessbeschreibung Datenschutzverletzung

Eine Datenschutzverletzung bedeutet einen Sicherheitsvorfall, der zur zufälligen oder unrechtmäßigen Zerstörung, zum Verlust, einer Änderung, unbefugten Offenlegung oder einem unbefugten Zugriff auf die übermittelten, gespeicherten oder anderweitig verarbeiteten personenbezogenen Daten führt. Der Auftragsverarbeiter hat den Auftraggeber bei Datenschutzverletzungen, die aus dessen Auftrag resultieren, proaktiv zu informieren und ihn bei der weiteren Bearbeitung zu unterstützen. Auch hier sollte der Auftragsverarbeiter grundlegende Zuständigkeiten und Prozesse etablieren, wie z.B., dass

- >> Verstöße gegen die Vorschriften zum Schutz personenbezogener Daten oder gegen **Weisungen des Verantwortlichen** erkannt und der Verantwortliche unverzüglich informiert wird,
- >> Datenschutzverletzungen zeitnah untersucht und Maßnahmen zur Schadensminimierung ergriffen werden können,

- >> Verantwortliche bei einer möglichen Meldung der Datenschutzverletzung an die Behörden und ggf. die betroffenen Personen unterstützt werden können,
- >> Kontroll- und Qualitätssicherungsmaßnahmen im Umgang mit Datenschutzverletzungen etabliert werden können.

Konkrete Vorgaben zur Gestaltung des Prozesses zur Meldung – potenzieller - Datenschutzverletzungen macht zum Beispiel die Verhaltensregel „Trusted Data Processor“.¹⁶

6. Nachweis der Pflichten aus Art. 28 DS-GVO und Unterstützung bzw. Mitwirkung bei Kontrollen

Zum Nachweis der Erfüllung der Pflichten aus Art. 28 DS-GVO empfiehlt es sich ein Auftragsmanagement (s. Kap. 5.2) zu etablieren, indem sowohl die allgemeinen Regelungen als auch die individuellen Regelungen mit dem jeweiligen Auftraggeber (Verantwortlichen) sowie mit den im Rahmen der Leistungserbringung eingesetzten Unterauftragnehmern dokumentiert sind.

Im Hinblick auf die Unterstützung von bzw. Mitwirkung bei Kontrollen des Verantwortlichen sollte der Auftragsverarbeiter proaktiv eigene Kontrollen und Überwachungen von Prozessen, vertraglichen Vereinbarungen mit Verantwortlichen und Unterauftragnehmern sowie technischen und organisatorischen Sicherheitsmaßnahmen etablieren und mit der Dokumentation der Durchführung und ggf. dem Ergreifen von Optimierungsmaßnahmen ggü. dem Verantwortlichen einen entsprechenden Nachweis erbringen.¹⁷

Der Auftragsverarbeiter sollte sich zudem darüber im Klaren sein, welche Kontroll- und Überwachungsmaßnahmen über den kommerziellen Dienstleistungsvertrag abgedeckt sind und welche Maßnahmen des Verantwortlichen ggf. zusätzlich zu bepreisen sind.

¹⁵ VfV, „Trusted Data Processor“, Kapitel 4.4.

¹⁶ VfV, „Trusted Data Processor“, Kapitel 4.5.

¹⁷ s. hierzu auch VfV, „Trusted Data Processor“, Kapitel 4.3
– Kontrolle von Unterauftragsverarbeitern – und Kapitel 4.7
– Eigenkontrolle.

7. Rückgabe / Löschung von Daten nach Vertragsende

Auch wenn sich die Lösch- bzw. Rückgabepflicht grundsätzlich an den Verantwortlichen richtet, hat der Auftragsverarbeiter i.d.R. Entscheidungsspielräume hinsichtlich der technischen und organisatorischen Maßnahmen. Beim Auftragsverarbeiter sollte in jedem Fall eine Dokumentation

- >> der technischen Umsetzung von Datenlöschungen /-rückgaben (ggf. auch bei etwaigen Unterauftragnehmern)
- >> des Nachweises der Durchführung von Löschungen /-rückgaben (ggf. auch bei etwaigen Unterauftragnehmern)
- >> von Kontrollen und Überprüfungen im Hinblick auf die Wirksamkeit der Löschroutinen (inkl. ggf. erfolgter Aktualisierungen)

vorhanden sein und entsprechende Prozesse sollten etabliert sein.



5. Pflichten aus dem Auftragsverarbeitungsverhältnis

5.1 Vertrag zur Auftragsverarbeitung

Der Verantwortliche und der Auftragsverarbeiter sind nach Art. 28 Abs. 3 DS-GVO verpflichtet, entsprechende Auftragsverarbeitungsverträge zu schließen¹⁸. Dies kann neben der Schriftform auch in elektronischer Form erfolgen (Art. 28 Abs. 9 DS-GVO).



Auch der Abschluss in elektronischer Form muss die zivilrechtlichen Anforderungen an einen Vertragsschluss erfüllen!

Der Auftragsverarbeitungsvertrag kann in einem umfassenden Vertrag, z.B. einen Dienstleistungsvertrag, eingebunden sein. Die die Einhaltung der DS-GVO betreffenden Vertragselemente sollten an einem Ort (z.B. in einem Anhang) eindeutig als solche gekennzeichnet sein.¹⁹

Verantwortlicher und Auftragsverarbeiter können einen individuellen Auftragsverarbeitungsvertrag aushandeln oder aber auf Standardvertragsklauseln zurückgreifen. Die EU-Kommission hat am 04.07.2021 ein Vertragsmuster zur Auftragsverarbeitung (Standardvertragsklauseln) veröffentlicht²⁰. Um seine Bindungswirkung zu entfalten, dürfen diese Vertragsklauseln an sich nicht verändert werden. Sie können allerdings in einen weiteren Vertrag eingebettet und um weitere Klauseln ergänzt werden. Es besteht die Verpflichtung, die

¹⁸ Zu den Anforderungen an den Vertragsschluss s. a. GDD-Praxishilfe DS-GVO – Mustervertrag zur Auftragsverarbeitung, S. 5 f. „3.Grundlage der Verarbeitung“.

¹⁹ EDPB Leitlinien Verantwortlicher und Auftragsverarbeiter in der DSGVO, Version 2.0, Juli 2021, Seite 38.

²⁰ https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors_en

Klauseln im Hinblick auf die tatsächliche Verarbeitung personenbezogener Daten zu konkretisieren.

In der praktischen Umsetzung werden mit dem konkreten AV-Vertrag die Anforderungen des Verantwortlichen mit dem Standard-Leistungsangebot des Auftragsverarbeiters abgeglichen, konkretisiert und ggf. geändert. Für den Auftragsverarbeiter ist es von elementarer Bedeutung, dass alle individuellen Regelungen mit dem Auftragsverarbeiter dokumentiert und in seinem Auftragsmanagementsystem implementiert sind. Nur so kann er die Einhaltung der Anforderungen kundenspezifisch in den Prozessen und Systemen gewährleisten und im Rahmen eigener Kontrollprozesse nachweisen.

Hinweise zur Vertragsgestaltung finden sich in der GDD-Praxishilfe DS-GVO „Mustervertrag zur Auftragsverarbeitung“. Weiter finden sich Vertragsmuster für spezielle Verarbeitungssituationen wie z.B. im Kontext des Gesundheitswesens²¹ oder der Datenträgervernichtung²².

5.2 Auftragsmanagement

Hinweis:

Grundsätzlich sollten im Vertrag zur Auftragsverarbeitung nicht einfach die Bestimmungen der DS-GVO wiederholt werden. Vielmehr sollte sie spezifische, konkrete Angaben dazu enthalten, wie die Vorgaben eingehalten werden und welches Sicherheitsniveau für die Verarbeitung personenbezogener Daten, die Gegenstand der Verarbeitung sind, erforderlich ist.

Im Rahmen des Auftragsmanagements geht es darum, sämtliche konkreten Vereinbarungen, die mit einem Verantwortlichen (Auftraggeber) vertraglich vereinbart wurden zu dokumentieren und nachzu-

halten. Im Wesentlichen handelt es sich dabei um die Dokumentation

- >> spezifischer Anforderungen bzw. Abweichungen von den Standardvorgaben/-prozessen/-sicherheitsmaßnahmen des Verantwortlichen (Auftraggebers) ggü. dem „Standardangebot“ des Auftragsverarbeiters,
- >> konkreter Funktionseinheiten und Personen beim Verantwortlichen und Auftraggeber sowie ggf. Unterauftragnehmern und/oder externen Stellen, die mit konkreten (Schnittstellen-)Aufgaben betraut sind,
- >> konkreter Maßnahmen (z.B. Weisungen, Meldungen, Kontrollen) je Verantwortlichem,
- >> von Kontrollpflichten des Verantwortlichen und dessen Wahrnehmung,
- >> der Löschung bzw. Rückgabe von Daten nach Vertragsbeendigung.

Sämtliche Veränderungen sowohl auf Seiten des Verantwortlichen als auf Seiten des Auftraggebers sind zeitnah zu pflegen. Im Rahmen des Datenschutzmanagements unterliegt auch das Auftragsmanagement einem kontinuierlichen Verbesserungsprozess.

²¹ s. GMDS Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG), Mustervertrag zur Auftragsverarbeitung, <https://gesundheitsdatenschutz.org/html/adv-vertrag.php> (letzter Abruf am 17.05.2022).

²² GDD-Ratgeber Datenschutzgerechte Datenträgervernichtung, 4. Aufl. 2019, S. 91 ff., <https://www.gdd.de/gdd-arbeitshilfen/gdd-ratgeber/datenschutzgerechte-datentraegervernichtung-4-aufl-2019-1> (letzter Abruf am 17.05.2022).



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.

Die Inhalte dieser Praxishilfe wurden im Rahmen des GDD-Arbeitskreises „DS-GVO Praxis“ erstellt unter Mitwirkung von:

- Uwe Bargmann (Berater Datenschutzmanagement)
- Thomas Müthlein (DMC - Datenschutz Management & Consulting, GDD-Vorstand)
- Yvette Reif, LL.M. (GDD-Geschäftsstelle)

Herausgeber:

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

Heinrich-Böll-Ring 10

53119 Bonn

Tel.: 0228 969675-00

Fax: 0228 969675-25

www.gdd.de

info@gdd.de

Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn

Stand:

Version 2.0 (Januar 2023)