Praxishinweise für Auftragsverarbeiter nach Art. 28 DS-GVO

Die Auftragsverarbeitung wird zukünftig über Art. 28 DS-GVO geregelt. Während die Norm teilweise bekannte Vorgaben an die Dienstleisterauswahl und die vertragliche Gestaltung stellt, enthält die DS-GVO an verschiedenen Stellen eigene Rechtspflichten für Auftragsverarbeiter. Diese Praxishinweise der GDD möchten Hilfestellungen für Auftragsverarbeiter geben, wie die gesetzlichen Vorgaben umgesetzt werden können.

Diese Praxishilfe besteht **in Ergänzung zur GGD Praxishilfe DS-GVO IV – Mustervertrag zur Auftragsverarbeitung.**

A. Einleitung

Art. 28 DS-GVO stellt die zentrale Norm für die Auftragsverarbeitung dar.[1] Beteiligte einer Auftragsverarbeitung sind der Verantwortliche und der Auftragsverarbeiter. **„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). Gem. Art. 4 Abs. 10 DS-GVO ist die Auftragsverarbeitung weiterhin dergestalt **privilegiert**, dass der Auftragsverarbeiter kein Dritter ist. Eine Beschränkung der Privilegierung auf den **EWR-Raum** erfolgt nicht. Auftragsverarbeiter im Drittland sind damit ebenfalls keine „Dritten“ für den Verantwortlichen.

B. 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**[2], 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 Auftragsvearbeitung hat,
- wie der Dienstleister durch den Auftraggeber überwacht wird
- die Expertise des Dienstleistes bei der Auftragsvearbeitung
- 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 einem der folgenden Punkte 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

[1] Im BDSGneu finden sich keine Regelungen und Vorgaben zur Ausgestaltung einer Auftragsverarbeitung i.S.d. DS-GVO.

[2] Weiterführende Hinweise der Artikel-29-Datenschutzgruppe in Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ vom 16.02.2010 (WP169).

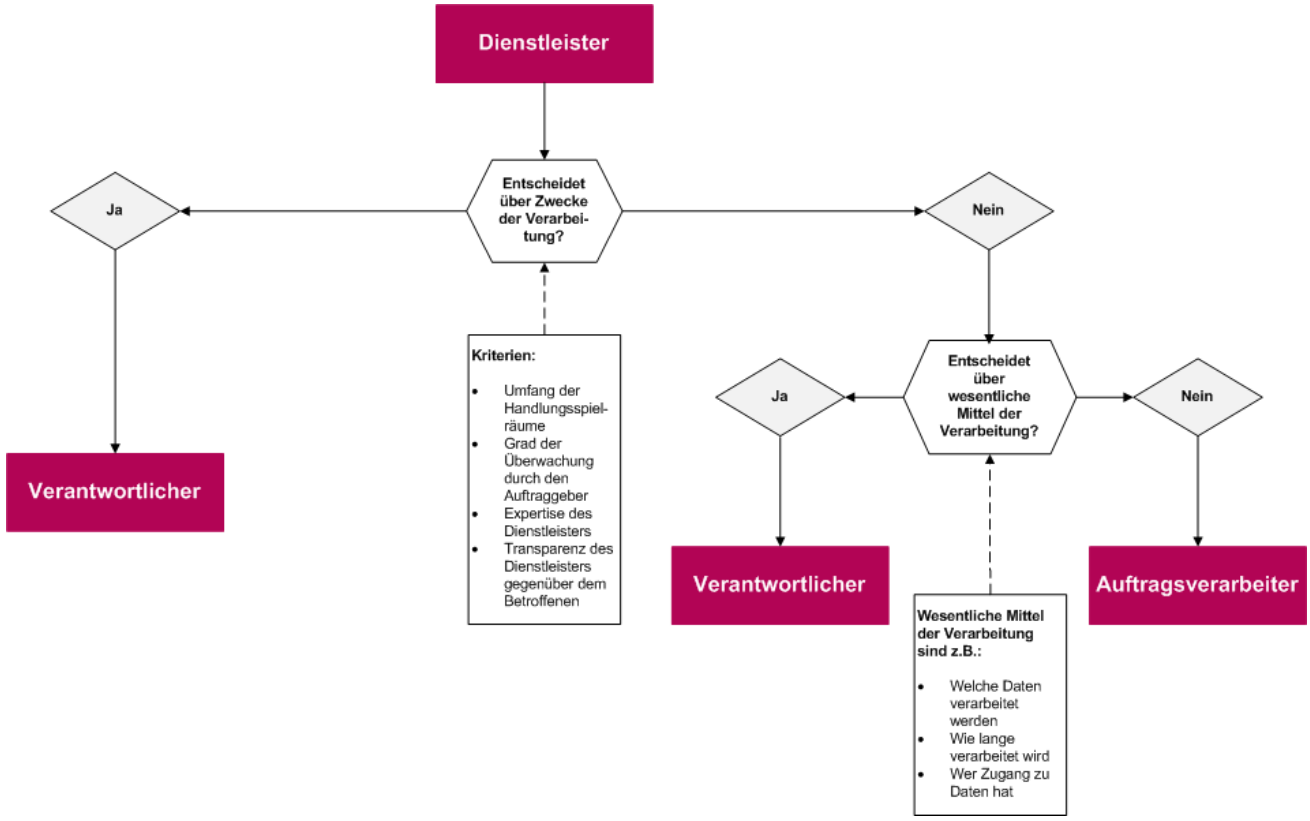
schwierig dar, so können verschiedene **Indizien**[3] für eine klarere Unterscheidung herangezogen werden:

- 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** für eine **Übermittlung** berücksichtigt werden;
- Hat der **Auftragnehme**r 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 Auftragsnehmers** für die **Richtigkeit** oder **Rechtmäßigkeit der Datenverarbeitung** in Frage, spricht auch dies eher für das Vorliegen einer Übermittlung.

Wird der Dienstleister mit der **IT-Wartung oder Fernwartung** betraut und besteht hierbei die Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten des Auftraggebers, soll es sich nach Meinung der hiesigen Aufsichtsbehörden um eine Form der Auftragsverarbeitung handeln und die Anforderungen des Art. 28 DS-GVO sollen für die geschuldete Tätigkeit gelten.[4] Bei einer rein technischen Wartung ohne Zugriff auf personenbezogene Daten des Auftraggebers gelten die Vorgaben des Art. 28 DS-GVO entsprechend nicht.

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

Abbildung 1: Einordnung Dienstleister



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

4 DSK Kurzpapier Nr. 13, S. 3.

Beispiele für Auftragsverarbeitungen sind:

- Cloud-Computing
- Newsletterversand
- Datenerfassung, Datenkonvertierung
- Auslagerung der Lohn- und Gehaltsabrechnung
- Backup-Auslagerung und Archivierung

Keine Auftragsverarbeitung stellen in der Regel dar:

- Tätigkeiten und damit verbundene Verarbeitungen personenbezogener Daten von Berufsgeheimnisträgern (Rechtsanwälte, Steuerberater[5], Wirtschaftsprüfer)
- Die Übertragung des Forderungsmanagements an ein Inkassounternehmen
- Postdienstleistungen in Form des Brieftransports

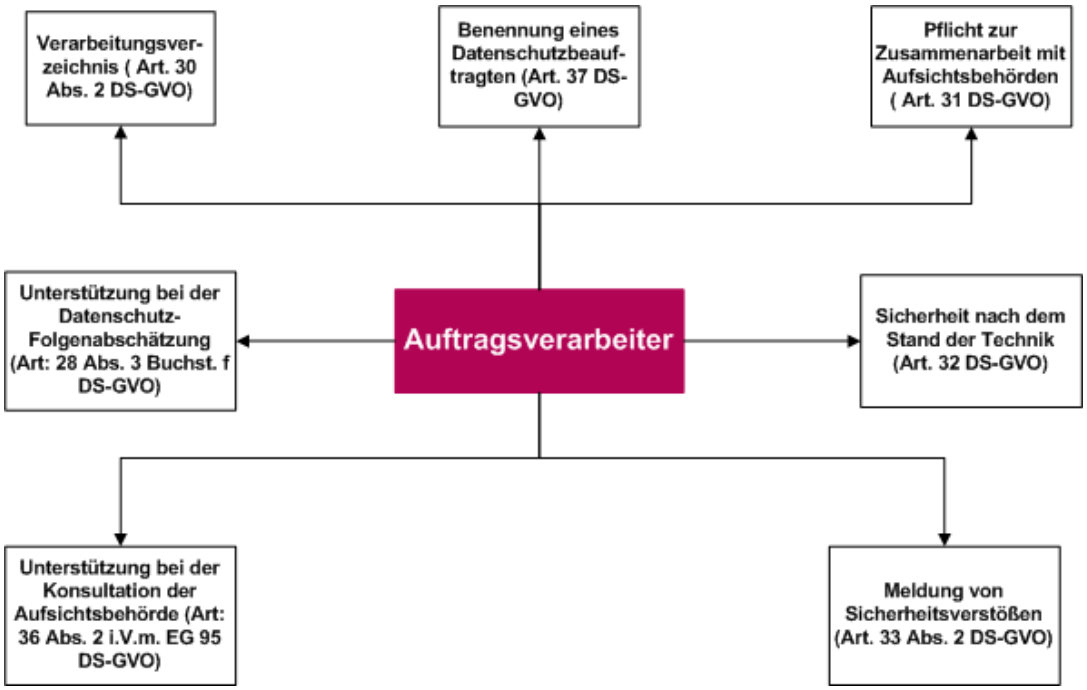
C. Verantwortlichkeiten in der DS-GVO

Durch die gesetzliche Abgrenzung zwischen Verantwortlichem und Auftragsverarbeiter bleibt es bei dem Grundsatz, dass der Verantwortliche grundsätzlich die Stelle ist, die über Zwecke und wesentlichen Mittel einer Datenverarbeitung entscheidet und für die **Rechtmäßigkeit der Verarbeitung** insgesamt verantwortlich ist (vgl. Art. 24 DS-GVO). Mit Anwendung der DS-GVO werden jedoch auch dem Auftragsverarbeiter **Rechtspflichten** auferlegt, die er als **Normadressat** zu erfüllen hat. Dies ist eine fundamentale Veränderung zur alten Rechtslage, in der die gesetzlichen Vorgaben grundsätzlich nur gegenüber dem Verantwortlichen durchgesetzt werden konnten.

D. Pflichten für Auftragsverarbeiter

Auftragverarbeitern werden in zahlreichen Normen eigene Rechtspflichten auferlegt:

Abbildung 2: Rechtspflichten für Auftragsverarbeiter



Neben eigenen Pflichten beinhaltet die DS-GVO Vorgaben für den Auftragsverarbeiter, um den Verantwortlichen bei der Einhaltung der gesetzlichen Vorgaben zu **unterstützen**. Diese Unterstützungspflichten sind entweder

[5] Das LDI NRW (http://t1p.de/ewvo) geht im Falle der reinen Lohn- und Gehaltsabrechnung oder bei sonstigen, rein technischen Dienstleistungen auch bei Steuerberatern von einer AV aus. Das BayLDA (http://t1p.de/82g6) hingegen sieht auch bei reiner Lohnbuchhaltung eine eigene Verantwortung der Steuerberater aufgrund des Steuerberaterrechts als gegeben an.

unmittelbar (vgl. Schaubild 2) oder mittelbar aus anderen gesetzlichen Normen der DS-GVO zu entnehmen.

Im Rahmen der Auswahl eines Auftragsverarbeiters haben Verantwortliche gemäß Art. 28 Abs. 1 DS-GVO darauf zu achten, dass dieser hinreichend **Garantien** dafür bietet, dass **geeignete technische und organisatorische Maßnahmen** so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Diese für eine sorgfältige Dienstleisterauswahl elementare Vorgabe ist durch die Implementierung technisch-organisatorischer Maßnahmen beim Auftragsverarbeiter zu konkretisieren. Die zu implementierenden Maßnahmen lassen sich modular aufbauen und können im Sinne einer Checkliste abgearbeitet werden[6]:

I. Leistungsbeschreibung

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

Die Leistungsbeschreibung ist die verbindliche Grundlage für die Gestaltung der Vertragsbeziehung zwischen Verantwortlichem und Auftragsverarbeiter und sorgt für die erforderliche **Transparenz der Datenverarbeitung**. Es bietet sich an, die Beschreibung an der jeweiligen Phase einer Beauftragung durch einen Auftraggeber zu orientieren. So werden in der **Auswahlphase** vereinfachte Darstellungen im Hinblick auf den Gegenstand und den Umfang, die Art und den Zweck der Datenverarbeitung sowie angemessener Datenschutz- und IT-Sicherheitsmaßnahmen ausreichend sein. In der **Vertragsphase** bieten sich Musterklauseln an, die auch auf konkrete IT-Sicherheitsmaßnahmen Bezug nehmen.

II. Beschreibung der Herstellung

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 Auftragsverarbeiter
- Qualitätssicherungsprozesse
- Maßnahmen hinsichtlich Privacy by Design and by Default

III. Input-Management

Datenweitergaben vom Verantwortlichen zum Auftragsverarbeiter in großem Umfang oder/und in hoher Regelmäßigkeit als Teil der Leistungserbringung sind umfassend zu dokumentieren. Eine Beschreibung der **Schutzmaßnahmen** und **Abläufe** der technischen Datenweitergabe vom Verantwortlichen zum Auftragsverarbeiter hat zu erfolgen, inkl. der Kontrolle und Annahmedokumentation. Bei Verwendung externer Datenquellen außerhalb der Sphäre des Verantwortlichen ist die Rechtsgrundlage für die Datenverarbeitung zu dokumentieren.

IV. Auftragsmanagement

Ein Nachweis über funktionierende **Schnittstellen** zwischen den an der Leistungserbringung beteiligten Stellen und die vollständige Kontrolle über den jeweiligen **Status** eines Auftrags stehen beim Auftragsmanagement im Vordergrund.

Der Auftragsverarbeiter hat den Nachweis zu erbringen, dass ein revisionssicheres Auftragsmanagement implementiert ist. Verbindlichkeit, Handlungssicherheit und aktueller Status für jeden Auftrag müssen bei allen Beteiligten jederzeit sichergestellt sein. Zu den Beschreibungen zählen

- Abläufe der Auftragsbearbeitung, einschließlich der Tätigkeiten von weiteren Auftragsverarbeitern und Dienstleistern
- Beschreibung von Rollen und Schnittstellen
- Änderungsprotokollierung für die Auftragsverarbeitung

[6] Vgl. hierzu ausführlich Datenschutzstandard „DS-BvD-GDD-02" für Auftragsverarbeiter gem. Art. 28 DS-GVO (Veröffentlichung voraussichtlich 2. Quartal 2018).

V. Output-Management

Werden Datenweitergaben vom Auftragsverarbeiter zum Verantwortlichen als Teil der Leistungserbringung definiert, kann durch ein Output-Management die Datenschutzkonformität der entsprechenden Prozesse geprüft werden. 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

- Abläufe der Datenübertragung beschrieben werden,
- ein Berechtigungskonzept erstellt werden,
- die Datenweitergabe protokolliert werden,
- IT-Anwendungen auf die Möglichkeit eines Datenexports überprüft werden.

VI. Datenschutzkonzept

Ein Datenschutzkonzept stellt die Erfüllung der gesetzlichen Vorgaben sicher. Elementare Bestandteile des Datenschutzkonzepts eines Auftragsverarbeiters sind:

1. Eingabekontrolle

Veränderungen an Daten des Auftraggebers müssen angemessen protokolliert werden. Die Protokolle werden regelmäßig stichprobenartig kontrolliert, ob Veränderungen an Daten der Auftraggeber von berechtigten Personen durchgeführt worden sind.

2. Trennung von Daten verschiedener Verantwortlicher

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.

3. 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)

4. Prozessbeschreibung Auskunft, Berichtigung, Datenübertragbarkeit und Löschung

Die Rolle des Auftragsverarbeiters hinsichtlich der Wahrung von Betroffenenrechten kann, je nach Auftrag, variieren.

Der Prozess beim Auftragsverarbeiter hat in jedem Fall **Unterstützungshandlungen** des für die Verarbeitung Verantwortlichen vorzusehen. Hierzu bedarf es eines **Datenschutzprozesses** beim Auftragsverarbeiter, der an den Prozess des Verantwortlichen zur Erfüllung der Betroffenenrechte angebunden werden kann. Der Prozess 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 entgegenzunehmen und unverzüglich an den zuständigen Verantwortlichen **weiterzuleiten** sind, es sei denn der Auftragsverarbeiter hat sich vertraglich zur Beauskunftung für den Verantwortlichen verpflichtet,
- alle berechtigten Begehren **zeitnah** und **vollständig** erfüllt werden können (technische Umsetzung). Dabei sind **Rechte Dritter** zu wahren, so dürfen z.B. im Rahmen eines Auskunftsbegehrens keine Daten anderer Personen, Mitarbeiter oder Verantwortlicher mitbeauskunftet werden,
- eine **Qualitätskontrolle** etabliert ist,
- im Falle von **veröffentlichten** personenbezogenen Daten weitere Verantwortliche über ein Löschbegehren eines Betroffenen informiert werden.

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. Auch hier hat der Auftragsverarbeiter den Auftraggeber bei Daten, die aus dessen Auftrag resultieren, zu unterstützen. Dies beinhaltet

- eine **Beschreibung**, wie der **Datenschutzprozess** des Auftragsverarbeiters an den entsprechenden Prozess des Verantwortlichen angebunden werden kann,
- die Existenz eines Prozesses, um Verstöße gegen die **Weisungen des Verantwortlichen** oder gegen die **Vorschriften zum Schutz personenbezogener Daten** zu erkennen und unverzüglich den Verantwortlichen zu informieren. Dazu gehören auch Sachverhalte, die geeignet sind, die Interessen des Verantwortlichen zu tangieren,
- die Existenz eines Prozesses, um Datenschutzverletzungen, die eine **gesetzliche Meldepflicht** auslösen können, zu erkennen, den Verantwortlichen unverzüglich zu informieren und Maßnahmen zur Schadensminimierung einzuleiten,
- die Existenz eines Prozesses, um eine Datenschutzverletzung zeitnah zu untersuchen und aufzuklären.

VII. IT-Sicherheitskonzept

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

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

Der Auftragsverarbeiter hat ein IT-Sicherheitskonzept basierend auf der angebotenen Leistung erstellt, das die Sicherheit der Auftragsdaten zum Gegenstand hat. Es erfüllt die Vorgaben zur Risikoabschätzung des Art. 32 Abs. 1 DS-GVO und folgt einem etablierten Standard (z.B. BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“).

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.

VIII. Datenschutz-Managementsystem

Da der Auftraggeber die datenschutzrechtliche Verantwortung für die unter seiner Verantwortung erhobenen personenbezogenen Daten trägt und den Auftragsverarbeiter mit der Verarbeitung dieser Daten beauftragt, erwächst für den Auftragsverarbeiter die Verpflichtung, seinerseits die Einhaltung von Datenschutzbestimmungen sicherzustellen. Das Datenschutz-Managementsystem ist ein Instrument, dieser Verpflichtung nachzukommen und orientiert sich an den Definitionen des **Datenschutzkonzepts**. Es beinhaltet u.a.

- die Bestellung eines **Datenschutzbeauftragten**,
- die Verpflichtung der mit der Datenverarbeitung befugten Personen des Auftragsverarbeiters auf einen vertraulichen Umgang mit Daten sowie ergänzende Schulungsmaßnahmen,
- die stichprobenhafte Kontrolle der angebotenen Leistung auf deren **Datenschutzkonformität,**
- einen Unterstützungsprozess zur **Datenschutz-Folgenabschätzung**, der an den entsprechenden Prozess des Verantwortlichen angebunden werden kann. Dies beinhaltet auch eine Unterstützung bei einer möglichen **Konsultation einer Aufsichtsbehörde** nach Art. 36 DS-GVO. Dieser Prozess schließt eine **dokumentierte Risikobewertung** hinsichtlich der Rechte und Freiheiten betroffener Personen ebenso mit ein, wie Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, um identifizierte Risiken zu bewältigen,
- einen Prozess zur **regelmäßigen Kontrolle** von weiteren Auftragsverarbeitern (Unterauftragnehmer), die für die Leistungserbringung wesentlich sind oder Zugriff auf Auftragsdaten erhalten.

IX. 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 ein Zertifikat möglich (vgl. Art. 42 DS-GVO).

X. Auftragsmanagementsystem

Das Modul Auftragsmanagementsystem stellt die Kontrolle des **weisungsgebundenen** Handelns des Auftragsverarbeiters in den Mittelpunkt. Hierdurch soll gewährleistet werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden (vgl. Art. 29 DS-GVO). Für ein Auftragsmanagementsystem ist folgendes elementar:

- Dokumentation von **Prozessen zur Auftragsbearbeitung** und deren Kontrolle,
- **Verpflichtung** der zur Verarbeitung befugten Personen auf **Vertraulichkeit,**
- Bearbeitung von Weisungen des Auftraggebers über einen Prozess (Change Management),
- **Information** des Verantwortlichen über eine Beauftragung weiterer Auftragsverarbeiter, das Einholen etwaiger **Genehmigungen** bzw. die Ermöglichung und Umsetzung von **Widersprüchen** des Verantwortlichen,
- die Ermöglichung angemessener **Prüfungen** durch den Verantwortlichen hinsichtlich der Auftragsbearbeitung.

XI. Vertrag zur Auftragsverarbeitung

Gemäß Art. 28 Abs. 9 DS-GVO kann ein Vertrag zur weisungsgebundenen Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter **schriftlich** oder in einem **elektronischen Format** abgefasst werden. Dieser Vertrag muss den Anforderungen des Art. 28 DS-GVO entsprechen.

Anregungen zur Vertragsgestaltung finden sich in der **GDD-Praxishilfe DS-GVO IV "Mustervertrag zur Auftragsverarbeitung"**.[7] Für Verträge im Kontext des Gesundheitswesens besteht ebenfalls ein Muster.[8]

XII. Beendigung der Leistungsbeziehung

Nach Beendigung eines Auftrages müssen klare **Regelungen** zwischen Auftragsverarbeiter und Verantwortlichem bestehen, was mit den beim Auftragsverarbeiter vorhandenen Daten geschehen soll (Löschung, Rückgabe, Archivierung oder Weiterverwendung im Rahmen eines Folgeauftrags). Es existiert ein **Prozess zur Auftragsbeendigung**, der auch das Löschen oder Zurückgeben der Auftragsdaten an den Verantwortlichen umfasst. Dies schließt sämtliche Daten bei etwaigen weiteren Auftragsverarbeitern mit ei

[7] https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_4.pdf (letzter Abruf am 01.02.2018)

[8] https://www.bvdnet.de/wp-content/uploads/2017/07/Muster-AV-Vertrag.doc (letzter Abruf am 01.02.2018).