**Hilfestellung zur Auftragsverarbeitung**

**1. Definition**

Auftrags(daten)verarbeitung (nach der DSGVO heißt diese nur noch Auftragsverarbeitung) liegt immer dann vor, wenn eigene Daten an andere Unternehmen, natürliche oder juristische Personen, Behörden oder sonstige Stellen **weiter gegeben** werden, um sie dort zu speichern oder sonst zu verarbeiten oder, wenn Dritten der Zugriff auf die eigene Datenverarbeitung gegeben wird und das weitergebende Unternehmen allein über die Zwecke und die Reichweite der Verarbeitung entscheidet.

Eine Auftragsverarbeitung nach [Art. 28 DSGVO](http://dejure.org/gesetze/DSGVO/28.html) ist also nur gegeben, wenn ein Dienstleister beauftragt wird, Daten **nach Weisung** des Auftraggebers zu verarbeiten und die **Verantwortung** für die Daten so bei dem Auftraggeber verbleibt.

**2. Weitergabe an Dritte, die nicht Auftragsverarbeitung ist**

Fehlt das Element der Weisung, bleibt die Verantwortung für die Daten nicht bei dem Auftraggeber. So werden IT-Hardwarewartungsunternehmen oder Logistiker nicht mit einer Datenverarbeitung beauftragt. Sie verarbeiten die Daten vielmehr nur im eigenen Interesse.

Mischfälle sind möglich bei der **Wartung** von Software. Hier war nach dem vorherigen deutschen Recht in § 11 Abs. 5 BDSG vorgesehen: „wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann“, liegt auch eine Auftragsverarbeitung vor. § 11 Abs. 5 BDSG gilt jedoch nicht mehr, dass vor allem eine Wartungstätigkeit, die sich nur auf die technische Komponente bezieht, ebenfalls keine Auftragsverarbeitung ist. Anders natürlich, wenn etwa auch eine Pflege von Daten Teil des Auftrages ist. Weil die Abgrenzung schwierig und auch die Rechtslage noch nicht eindeutig geklärt ist, empfiehlt es sich, vorsichtshalber einen Auftragsverarbeitungsvertrag mit dem Wartungsunternehmen zu schließen.

Keine Auftragsdatenverarbeitung ist auch die Inanspruchnahme fremder **Fachleistungen** wie Inkasso, Rechtsanwalt, Steuerberater. Dies gilt vor allem für klassische Freiberufler, primär auch solche, die zur Berufsverschwiegenheit verpflichtet. Diese sind zudem auch nicht im engeren Sinne weisungsgebunden.

In diesen Fällen ist keine Auftragsverarbeitung gegeben, vielmehr handelt es sich bei dieser **Weitergabe von Daten** (für eigene Zwecke des dritten Unternehmens) um eine normale Datenverarbeitung (die eben auch die Weitergabe der Daten an Dritte umfasst). Diese bedarf also einfach einer **Erlaubnisnorm**, muss sich also auf einen der Gründe des [Art.6 Abs.1 DSGVO](http://dejure.org/gesetze/DSGVO/6.html) zurück führen lassen (häufigster Fall wird die Verarbeitung von Vertragsdaten sein, aber es kommen auch berechtigte Interessen oder eine Einwilligung in Betracht).

**Ergebnis**

Auftragsdatenverarbeitung ist also nur gegeben, wenn sich der Auftrag auf eine Arbeit grade mit den Daten nach Weisung des Auftraggebers bezieht.

Es kann sich aber für den Fall von Abgrenzungsproblemen empfehlen, wenigstens **vorsorglich** zusätzlich noch einen Auftragsverarbeitungsvertrag zu schließen.

**2. Abgrenzung**

Abzugrenzen ist sie in zweierlei Hinsicht:

* von der **eigenen Datenverarbeitung**, also, wenn nur eigene Angestellte die Daten verarbeiten, das ist noch eigene Datenverarbeitung und nicht Datenverarbeitung durch Dritte (wie man eigene Mitarbeiter zu den Anforderungen der DSGVO verpflichtet, findet sich [hier](https://www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf) mit entsprechenden Mustern);
* von der **gemeinsamen Verantwortung** für die Datenverarbeitung gem. Art. 26 DSGVO, bei der komplette Funktionen an Dritte ausgelagert werden und diese eigene Entscheidungskompetenzen für die Daten haben (Bsp. Stellung der Personalabteilung durch die Konzernmutter)

**3. Ergebnis für Websites und Online-Unternehmen**

Typische Fälle einer Auftragsverarbeitung für Websites und Online-Unternehmen sind also:

* Mail (Newsletter) Anbieter
* Hoster (wenn bei diesem personenbezogene Daten gespeichert werden, zB eine Datenbank)
* Cloud Anbieter
* SaaS Anbieter
* Agentur macht Werbung
* Buchhaltung
* Tracking Software – Beispiel Google Analytics
* Einsatz virtueller Assistenten (je nach Auftragsumfang)

**4. Rechtsfolge**

a) unmittelbare Rechtsfolge

Unmittelbar hat das Vorliegen einer Auftragsdatenverarbeitung zur Folge, dass gem. Art. 28 Abs. 3 DSGVO ein **Vertrag zur Auftragsverarbeitung** erforderlich ist. Die Inhalte können dort nachgelesen werden.

b) sich ergebende Anforderung

Weitere Rechtsfolge ist aber, dass der Auftraggeber gem. Art. 28 Abs. 1 DSGVO den Auftragsverarbeiter ordnungsgemäß **auszusuchen** und zu **überwachen** hat. Es darf nur jemand ausgesucht werden, der hinreichende Gewähr für die Einhaltung der Anforderungen der DSGVO bietet.

c) wichtige Konsequenz

Ganz wichtig ist zu verstehen, dass die Auftragsdatenverarbeitung die wesentliche Rechtsfolge hat, dass durch die **Auftragsdatenverarbeitung keine Weitergabe** von Daten **an einen Dritten** mehr vorliegt. Man braucht dafür also nicht noch mal einen der Gründe aus Art. 6 DSGVO (insbesondere Vertragsdaten, Einwilligung oder berechtigtes Interesse), sondern kann im Rahmen der eigenen Erlaubnis aus Art. 6 DSGVO die Daten weitergeben.

Insofern gibt es teilweise ein Wahlrecht, man kann entweder den Nutzer in die Weitergabe der Daten an einen Dritten einwilligen lassen oder kann einen Vertrag zur Auftragsdatenverarbeitung mit dem Dritten schließen.

**5. Neuerungen durch die DSGVO**

Im Grundsatz bringt die DSGVO wenig Neues

* Auftragsverarbeiter muss jetzt auch Verarbeitungsverzeichnis führen
* Auftragsverarbeiter muss Weisungen protokollieren vom Auftraggeber
* Schriftform ist nicht mehr erforderlich.

Wie bei allen Datenschutz-Themen gilt aber auch hier, dass die Durchsetzung der Anforderungen jetzt verstärkt und mit mehr und teureren Konsequenzen zu erwarten ist.

**6. Der Vertrag**

Ihr müsst einen Auftragsverarbeitungsvertrag daher einerseits mit allen Dritten abschließen, die Eure Daten oder Daten Eurer Kunden verarbeiten. Dieser wird von vielen Dienstleistern – zB Google – bereits angeboten. Bei englischsprachigen Dienstleistern nach **data processing agreement** suchen. Eine umfangreiche Übersicht über angebotene Verträge von vielen Dienstleistern und wo sie zu finden sind findet sich [hier](https://www.blogmojo.de/adv-vertraege/).

Ihr müsst aber auch Euren Kunden einen Auftragsverarbeitungsvertrag anbieten, wenn Ihr Auftragsverarbeiter im Sinne der oben genannten Definition seid. Dafür ist das beigefügte Muster.

Der Vertrag ist immer die Anlage zu dem Vertrag, den ihr in der Hauptsache mit dem Auftraggeber oder Auftragnehmer schließt (es kommt immer darauf an, wer in der **Verantwortung für die Daten** bleibt),

**7. Besondere technische und organisatorische Maßnahmen**

Damit Ihr einen besseren Überblick bekommt, welche Schutzmaßnahmen im Anhang noch genannt werden können, habe ich Euch weiter eine Datei mit einer möglichen Liste der technischen und organisatorischen Schutzmaßnahmen (TOM) beigefügt. Je größer Dein Unternehmen, desto eher sind solche Maßnahmen erforderlich.

Kleinere Unternehmen können sich auf die Nennung von Passwortschutz, Zutrittskontrolle und Verschlüsselung beschränken, müssen also nicht umfangreiche Eintragungen machen (es gab aber auch schon Fälle, in denen größere Auftraggeber die Maßnahmen als zu gering zurückgewiesen haben).