



Frage	Was ist Auftragsverarbeitung und was nicht?
Norm	Art. 4 Nr. 8 und Art. 28 DS-GVO
Stichworte	Auftragsverarbeitung, Abgrenzung
Antwort	<p>Ob ein Dienstleister, der bei der Erbringung seiner Dienstleistung personenbezogene Daten verarbeitet, als Auftragsverarbeiter oder aber als Verantwortlicher (oder ggf. als gemeinsam Verantwortlicher mit dem „Auftraggeber“) einzustufen ist, gehört zu den Fragen, die in der Praxis des Datenschutzes am häufigsten gestellt werden.</p> <p>Auftragsverarbeiter ist nach Art. 4 Nr. 8 DS-GVO eine Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Auftragsverarbeitung liegt somit nur in Fällen vor, in denen eine Stelle von einer anderen Stelle mit der Verarbeitung personenbezogener Daten beauftragt wird.</p> <p>In einer früheren Veröffentlichung hatten wir an dieser Stelle einen umfangreichen Katalog von Dienstleistungen aufgezählt und diese - zumindest für den „Durchschnittsfall“ - in die Kategorien Auftragsverarbeitung bzw. eigenständige Verantwortlichkeit eingeordnet. Was als einfache Abgrenzungshilfe gedacht war, hat jedoch in der Praxis allzu oft Fragen aufgeworfen. Grund hierfür war vor allem, dass hinter ein und demselben Schlagwort, mit dem in der Praxis Dienstleistungen beschrieben werden, sehr unterschiedlich gestaltete Datenverarbeitungsprozesse stecken können. Wenn die gesetzlichen Merkmale für Verantwortlichkeit und Auftragsverarbeitung auf derart unterschiedliche Verarbeitungsprozesse zutreffend angewendet werden, können je nach Einzelfall durchaus unterschiedliche datenschutzrechtliche Rollenbestimmungen das Ergebnis sein, selbst wenn in der „Business-Sprache“ für die entsprechenden Dienstleistungen bisweilen ein gleichlautender Begriff gebräuchlich ist. Vor diesem Hintergrund haben wir uns dazu entschlossen, fortan keinen Tätigkeitskatalog mit entsprechenden datenschutzrechtlichen Rolleneinordnungen mehr zu veröffentlichen, sondern die gesetzlichen Kriterien für die zutreffende Einordnung näher zu erläutern.</p> <p>Anwender sind darauf angewiesen, für die korrekte Bestimmung der datenschutzrechtlichen Rollen als Verantwortlicher, Gemeinsam Verantwortliche oder aber Auftragsverarbeiter die gesetzlichen Definitionen auf den einzelnen Fall korrekt anzuwenden. Hierzu geben die Ausführungen des Europäischen Datenschutzausschusses / EDSA in den Leitlinien 7/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0 vom 07.07.2021 (https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_de) umfangreiche Hilfestellungen.</p> <p>Verantwortlicher ist gemäß Art. 4 Nr. 7 DSGVO, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Auftragsverarbeiter ist gemäß Art. 4 Nr. 8 DSGVO, wer personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.</p> <p>Das maßgebliche Merkmal, das eine Stelle zum datenschutzrechtlich Verantwortlichen macht, ist somit die „Entscheidung über die Zwecke und Mittel der Verarbeitung personenbezogener Daten“. Wer diese Entscheidung nicht trifft, ist kein Verantwortlicher. Diese gesetzlichen Merkmale sind auch in Fällen der Inanspruchnahme externer Dienstleistungen anzuwenden, um die datenschutzrechtlichen Rollen von Dienstleister und Dienstleistungsempfänger zu bestimmen.</p> <p>Nicht jeder Dienstleister, der im Zuge seiner Leistungserbringung personenbezogene Daten verarbeitet, ist Auftragsverarbeiter. Ein hilfreicher Ausgangspunkt für die Bestimmung der</p>

datenschutzrechtlichen Rollen der Beteiligten ist jedoch in jedem Falle zunächst **die Art der Dienstleistung**. Auftragsverarbeitung liegt in den Worten des EDSA (Leitlinien 07/2020, Rn. 82) in der Regel *jedenfalls dann* vor, wenn

- die Dienstleistung ihrem Inhalt nach speziell auf die Verarbeitung personenbezogener Daten abzielt, oder
- die Verarbeitung personenbezogener Daten ein Schlüsselement der Dienstleistung darstellt.

Die EDSA-Leitlinien nennen hierzu unter anderem folgende Beispiele:

- Hosting/Speicherung personenbezogener Daten nach Weisung (selbst wenn die Daten verschlüsselt sind; Rn. 40 EDSA-LL 7/2020)
- Cloud-Dienstleistungen wie Messaging, Videokonferenzen, Dokumentenspeicherung, Kalenderverwaltung, Textverarbeitung u.a. durch einen Dienstleister (Rn. 84 EDSA-LL).

Als Auftragsverarbeitung sind aber auch Dienstleistungen einzuordnen, die nach ihrem Hauptgegenstand bzw. ihrem Inhalt **zwar nicht auf die Verarbeitung von personenbezogenen Daten abzielen, jedoch einen systematischen, umfangreichen Zugang zu personenbezogenen Daten unvermeidlich** mit sich bringen. Der EDSA nennt als Beispiel:

- Beauftragung eines IT-Dienstleisters mit dem allgemeinen Support von IT-Systemen, wenn hierbei (wie häufig) der *systematische* Zugang zu personenbezogenen Daten faktisch möglich ist (Rn. 83 EDSA-LL 7/2020)
 - Anders aber laut EDSA, wenn ein IT-Berater *in einem Einzelfall* – d.h. ohne ein dauerhaftes Betreuungsverhältnis zum Auftraggeber zu haben – engagiert wird, um ein Problem zu beheben und dabei (wie häufig) rein beiläufig (EDSA: „zufällig“; engl.: incidental) Zugang zu personenbezogenen Daten erhält; der Berater soll laut EDSA hier kein Auftragsverarbeiter sein; Abgrenzungskriterium ist somit, dass es sich in diesem Fall nicht um eine systematische, dauerhafte Datenzugangsmöglichkeit handelt, sondern um einen Einzelfall.
 - Laut EDSA ist der IT-Berater in diesem Fall auch nicht als Verantwortlicher einzuordnen; dahinter steht die Überlegung, dass der Berater in einem solchen Fall bezogen auf die Daten keine „Verarbeitung“ durchführt.

Achtung: „Funktionsübertragung“ gibt es unter der DSGVO nicht (mehr)!

Auftragsverarbeitung kommt aber **nicht ausschließlich in den oben genannten Fällen** in Betracht. In der Zeit vor Geltungsbeginn der DSGVO war in Deutschland das Konzept der sog. Funktionsübertragung gebräuchlich. Nach diesem Konzept wurden Dienstleistungen, deren Schwerpunkt nicht in der Verarbeitung personengezogener Daten liegt, nicht als Auftragsverarbeitung eingestuft, vielmehr wurde der Dienstleister dann in aller Regel als Verantwortlicher gewertet. Dieses Konzept kann so nicht aufrechterhalten werden, da es in der DSGVO keine Stütze findet. Vielmehr kann es **im Einzelfall Auftragsverarbeitung auch in Fällen geben, in denen der vorrangige Gegenstand einer Dienstleistung nicht auf die Verarbeitung personenbezogener Daten abzielt** (EDSA-Leitlinien/LL 7/2020, Randnummer/Rn. 83), nämlich dann, sofern es „dennoch“ der Auftraggeber/Empfänger der Dienstleistung ist, der die Entscheidung über die Zwecke und Mittel der Verarbeitung trifft. Der EDSA nennt hierfür u.a. folgende Beispiele:

- Kundenbetreuung im Call-Center; die Kundenbetreuung bringt es mit sich, dass der Dienstleister Zugang zu den Kundendatenbanken des Auftraggebers benötigt (Rn. 83 EDSA-LL 7/2020)

- Marktforschungsinstitut, das im Auftrag und gemäß Anweisungen eines Produktherstellers eine Marktumfrage durchführt (Rn. 45 EDSA-LL 7/2020)
 - anders aber, wenn das Marktforschungsinstitut eine eigene Datenbank hat, die es nach eigener Methodik (d.h. nicht nach Weisungen eines Auftraggebers) erhoben hat und auswertet - dann ist das Marktforschungsinstitut Verantwortlicher
- Lohnbuchhaltung gemäß Anweisungen eines Arbeitgebers (Rn. 40 EDSA-LL 7/2020)

Obwohl in diesen Beispielfällen die Verarbeitung personenbezogener Daten nicht der „eigentliche“ bzw. Hauptgegenstand der Dienstleistung ist, sind sie laut EDSA als Auftragsverarbeitung einzustufen, da Zugang zu personengezogenen Daten stattfindet, die Entscheidung über die Zwecke und Mittel der Verarbeitung jedoch nicht vom Dienstleister, sondern vom Auftraggeber/Empfänger der Dienstleistung getroffen wird.

Einzuräumen ist, dass in Fällen der Inanspruchnahme von Dienstleistungen bei der Betrachtung der Frage, welcher der Beteiligten die Entscheidung über die Zwecke und Mittel der Verarbeitung trifft, auch gewisse Elemente der Perspektive und Wertung eine Rolle spielen mögen. Für die Datenschutzpraktiker ist es jedenfalls entscheidend, die Kriterien des EDSA zu kennen und sich die Einordnung des konkreten Praxisfalls anhand dieser Kriterien zuzutrauen.

Letztlich ist immer eine Einzelfallprüfung vorzunehmen um festzustellen, welcher Beteiligte in einem bestimmten Szenario Einfluss auf die Zwecke und Mittel der Verarbeitung hat, d.h. über die Zwecke und Mittel (mit)entscheidet und daher als Verantwortlicher einzustufen ist. Eine Abgrenzung wie in der Vor-DSGVO-Zeit allein anhand des Merkmals „Schwerpunkt der Dienstleistung“ ist unter der DSGVO jedenfalls nicht mehr möglich.

Nähere Informationen finden sich in den Leitlinien 7/2020 des EDSA (Version 2.0 vom 7.7.2021), abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_de