Begleitende Hinweise zu der Anlage der Auftragsverarbeitung

Leitfaden

bitkom

Inhalt

Vorwort

Die aktualisierte Version 1.2 des begleitenden Leitfadens zu der Anlage zur Auftragsverarbeitung wurde im November 2025 auf Grundlage der EU-Datenschutz-Grundverordnung (2016/679) erstellt und ersetzt den bisherigen Leitfaden.

Dieser Leitfaden dient als Orientierungshilfe und Erläuterung zur ebenfalls überarbeiteten Bitkom-Mustervertragsanlage zur Auftragsverarbeitung (Version 1.3 – 2025). Er soll Verantwortliche und Auftragsverarbeitende gleichermaßen dabei unterstützen, die datenschutzrechtlichen Anforderungen praxisgerecht umzusetzen und ein gemeinsames Verständnis der wesentlichen Regelungsinhalte zu fördern.

Für die Überarbeitung danken wir insbesondere den Mitgliedern des Arbeitskreises Datenschutz, die am Ende dieses Leitfadens namentlich aufgeführt sind.

Der Arbeitskreis Datenschutz setzt sich aus Expertinnen und Experten der Bitkom-Mitgliedsunternehmen zusammen und beschäftigt sich fortlaufend mit aktuellen Fragestellungen und Entwicklungen im Bereich Datenschutz.

Definitionen

Personenbezogene Daten

»Personenbezogene Daten« sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DS-GVO)

Auftragsverarbeiter

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DS-GVO)

Datenverarbeitung im Auftrag

Es gibt keine Legaldefinition der Auftragsverarbeitung in der DS-GVO. Artikel 28 DS-GVO legt lediglich die Anforderungen fest, die bei dieser Art der arbeitsteiligen Datenverarbeitungen bestehen. Demnach ist eine Datenverarbeitung im Auftrag die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter (Auftragnehmer) nach Weisung und im Auftrag des Verantwortlichen (Auftraggeber)

Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (z. B. Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt. Der Auftraggeber hat ein Weisungsrecht im Rahmen dieser vereinbarten Leistung.

Unterauftragsverarbeiter

Als Auftragnehmer des Auftragsverarbeiters im Sinne der DS-GVO ist der Subunternehmer ein »weiterer Auftragsverarbeiter«. Im Rahmen dieser sogenannten Unterauftragsverarbeitung sind die Vorgaben des Art. 28 Abs. 4 DS-GVO zu beachten.

Dritter

Der Ausdruck Dritter bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten (Art. 4 Nr. 10 DS-GVO).

1 Einleitung

Die fortschreitende Entwicklung der Dienstleistungsgesellschaft hin zu stärkerer Arbeitsteilung hat die Auftragsverarbeitung zu einem zentralen Bestandteil moderner Geschäftsprozesse gemacht.

Nach Art. 4 Nr. 8 DS-GVO ist der Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die personenbezogene Daten im Auftrag der Verantwortlichen (Auftraggeber) verarbeitet.

Das maßgebliche Kennzeichen – und zugleich Abgrenzungskriterium zu anderen Rechtsbeziehungen, wie etwa der gemeinsamen Verantwortlichkeit oder der Datenübermittlung – ist die in Art. 29 DS-GVO verankerte Weisungsgebundenheit des Auftragsverarbeiters gegenüber dem Verantwortlichen.

Gemäß Art. 28 Abs. 10 DS-GVO verstößt ein Auftragsverarbeiter gegen die Verordnung, wenn er über die Weisungen des Verantwortlichen hinausgeht und beginnt, eigene Zwecke oder Mittel der Verarbeitung zu bestimmen. In diesem Fall gilt der Auftragsverarbeiter in Bezug auf diese Verarbeitung als Verantwortlicher und kann für die Überschreitung der Weisungen mit Sanktionen belegt werden.

Typische Anwendungsfälle der Auftragsverarbeitung sind etwa IT-Outsourcing, der Betrieb von Rechenzentren, Software-as-a-Service (SaaS), Cloud Computing, der Betrieb von Onlineshops und Webhosting-Diensten, die Nutzung externer Lohn- und Gehaltsabrechnungsdienste sowie die Beauftragung externer Kundensupport- oder Callcenter-Dienstleister.

Die Auftragsverarbeitung ist in Art. 28 DS-GVO geregelt, ergänzend sind für das Verständnis der Auftragsverarbeitung die Erwägungsgründe 79, 81, 91 und 101, sowie die Art. 26, 79 und 82 DS-GVO heranzuziehen.

2 Wann liegt eine Auftragsverarbeitung vor?

Wenn personenbezogene Daten nicht ausschließlich von der verantwortlichen Stelle (selbst) verarbeitet werden, sondern eine weitere rechtlich eigenständige rechtliche Einheit beteiligt ist, kommen drei grundsätzliche Konstellationen in Betracht. Diese unterscheiden sich hinsichtlich ihrer formalen Anforderungen und materiellen Rechtmäßigkeitsvoraussetzungen.

Auftragsverarbeitung	Gemeinsame Verantwortlichkeit (Joint Controllership)	Übermittlung
Erlaubnistatbestand für Verarbeitung durch die verantwortliche Stelle + Vertrag/sonstiges Rechtsinstrument gemäß Art. 28 Abs.3 DS-GVO als Rechtmäßigkeitsvoraussetzung für Verarbeitung durch den Auftragsverarbeiter	Erlaubnistatbestand für Verarbeitung durch beide verantwortliche Stellen + Verarbeitung gemäß Art. 26 DS-GVO zur Verteilung der Pflichten	Erlaubnistatbestand für die Übermittlung von einem Verantwortlichen an einen anderen + Erlaubnistatbestand für Verarbeitung bei der empfangenden verantwortlichen Stelle.

2.1 Abgrenzung – Auftragsverarbeitung – sonstige Dienstleistungsverhältnisse

Als gesetzliche Grundlage tritt Art. 28 Abs. 1 DS-GVO immer dann in Kraft, wenn »eine Verarbeitung im Auftrag eines Verantwortlichen durch einen Auftragsverarbeiter erfolgt.«

Der Anwendungsbereich setzt also vier Elemente voraus:

1. Personenbezogene Daten werden verarbeitet (Art. 4 Nr. 1 DS-GVO).
2. Diese Verarbeitung erfolgt nicht durch den Verantwortlichen selbst, sondern im Auftrag des Verantwortlichen (Art. 28 Abs. 1 Satz 1 DS-GVO).
3. Die Verarbeitung erfolgt durch einen Auftragsverarbeiter und damit nicht durch den Verantwortlichen.

4. Der Auftragsverarbeiter verarbeitet ausschließlich auf Weisung des Verantwortlichen – also nicht zu eigenen Zwecken.

Nicht jede Tätigkeit mit Berührung zu personenbezogenen Daten stellt automatisch eine Auftragsverarbeitung im Sinne des Art. 28 DS-GVO dar. Maßgeblich ist, ob der Dienstleister durch den Verantwortlichen ausdrücklich mit der Verarbeitung personenbezogener Daten im Sinne einer weisungsgebundenen Datenverarbeitung im Auftrag betraut wird.

In bestimmten Fallkonstellationen kann die Verarbeitung personenbezogener Daten lediglich ein untergeordneter, beiläufiger Bestandteil der Leistung sein, der nicht den Schwerpunkt der Tätigkeit bildet. In solchen Fällen kann eine Auftragsverarbeitung zu verneinen sein.

Dies entspricht auch der Auffassung verschiedener Datenschutzaufsichtsbehörden. So heißt es beispielsweise in den FAQs zur Auftragsverarbeitung nach Art. 28 DS-GVO der LDA Niedersachsen:[1]

> »Kann es besondere Konstellationen geben, in denen ausnahmsweise keine Auftragsverarbeitung vorliegt, weil die Datenverarbeitung nur ein 'ungewolltes Beiwerk' einer (Haupt-)Dienstleistung darstellt? Ja. Nach Sinn und Zweck des Artikels 4 Nummer 8 in Verbindung mit Artikel 28 Absatz 1 DS-GVO kann in Einzelfällen eine Auftragsverarbeitung verneint werden, wenn die Datenverarbeitung lediglich im Zusammenhang mit der Erbringung einer (Haupt-)Dienstleistung für einen anderen erfolgt. Gemäß Erwägungsgrund 81 zur DS-GVO muss der Verantwortliche den Auftragsverarbeiter mit der Verarbeitung von personenbezogenen Daten 'betrauen wollen'. Dieses kann im Einzelfall verneint werden, wenn die Datenverarbeitung nicht speziell beabsichtigt ist beziehungsweise nicht den Schwerpunkt oder einen wichtigen (Kern-)Bestandteil der Leistung des Auftragnehmers darstellt.«

Beispiele für solche Konstellationen sind u. a.:

Ein Copyshop, der den Auftrag erhält, T-Shirts mit Namen zu bedrucken: Der Schwerpunkt der Leistung liegt auf dem farblichen Bedrucken der Textilien, nicht auf der Verarbeitung der Namen.

Ein Blumen- oder Weinhändler, der zum Zweck der Geschenkversendung eine Liste mit Adressdaten erhält: Die Datenverarbeitung dient lediglich der logistischen Abwicklung.

[1] LDA Niedersachsen, FAQ-Auftragsverarbeitung nach Artikel 28 DS-GVO, Frage Nr.4 , abrufbar unter: https://www.lfd.niedersachsen.de/startseite/infothek/faqs_zur_ds_gvo/faq-auftragsverarbeitung-189637.html#2 zuletzt abgerufen am:31.10.1025.

Ein Hersteller, der für Direktlieferungen vom Online-Händler die Kundendaten zur Zustellung erhält: Die personenbezogenen Daten sind erforderlich, um die Lieferung zu ermöglichen, stehen aber nicht im Zentrum der Leistung.

IT-Supportleistungen, bei denen etwa im Rahmen eines Ticketingsystems Kontaktdaten oder vereinzelt andere personenbezogene Inhalte übermittelt werden, die aber nicht Gegenstand der Dienstleistung sind.

In diesen Fällen kann es ausreichend sein, geeignete Vertraulichkeitsvereinbarungen zu treffen, ohne dass eine vollständige Auftragsverarbeitungsvereinbarung erforderlich ist

> Hinweis: Die Einordnung, ob eine Auftragsverarbeitung vorliegt, ist stets einzelfallbezogen vorzunehmen und hängt vom tatsächlichen Umfang und Zweck der Datenverarbeitung ab.

2.3 Abgrenzung Übermittlung – Auftragsverarbeitung

Von einer Übermittlung zwischen Verantwortlichen spricht man, wenn eine verantwortliche Stelle personenbezogene Daten an eine andere, eigenständig verantwortliche Stelle zugänglich macht oder übermittelt. Eine Übermittlung kann also nicht nur durch die Weitergabe von Daten erfolgen, sondern auch durch das Einräumen eines Zugriffs, z. B. im Rahmen von Wartungs-, Support- oder Hosting-Tätigkeiten. Beide Stellen verarbeiten die Daten für eigene Zwecke und unterliegen damit jeweils eigenen Verantwortlichkeiten im Sinne der DS-GVO.

Abgrenzung zur Auftragsverarbeitung

Eine Übermittlung ist somit keine Auftragsverarbeitung, da der Empfänger der Daten nicht weisungsgebunden handelt, sondern eigenständig über Zwecke und Mittel der Verarbeitung entscheidet. Grundlage für die Rechtmäßigkeit einer Übermittlung ist ein Erlaubnistatbestand sowohl für die Weitergabe durch den übermittelnden Verantwortlichen als auch für die anschließende Verarbeitung durch den empfangenden Verantwortlichen.

Beispiel für eine gesetzlich vorgeschriebene Übermittlung:

Ein Unternehmen übermittelt Daten von Beschäftigten oder Kunden an eine Behörde, um eine gesetzliche Verpflichtung zu erfüllen. Die Behörde verarbeitet die Daten anschließend zur Erfüllung ihrer eigenen gesetzlichen Aufgaben. Dabei verfolgt das Unternehmen seinen Zweck (z. B. Art. 6 Abs. 1 lit. c DSGVO), die Behörde ihren eigenen

(z. B. Art. 6 Abs. 1 lit. e DSGVO). Eine gemeinsame Zweckfestlegung zwischen beiden Stellen findet nicht statt; beide sind für ihre jeweiligen Datenverarbeitungen allein und getrennt verantwortlich.[2]

Weitere Praxisbeispiele:

- Eine Arztpraxis übermittelt Patientendaten an ein medizinisches Labor, das die Proben selbständig analysiert und die Ergebnisse in eigener Verantwortung verarbeitet.
- Ein Autohaus leitet Kundendaten an eine Versicherung weiter, um dem Kunden ein ergänzendes Versicherungsangebot zu unterbreiten. Beide Stellen verfolgen eigene Zwecke.
- Ein Unternehmen übermittelt Beschäftigtendaten an eine Krankenkasse oder eine Behörde, weil dies gesetzlich vorgeschrieben ist. Die empfangende Stelle verarbeitet die Daten eigenverantwortlich.

2.4 Abgrenzung Gemeinsam Verantwortliche (Joint Controllership) – Auftragsverarbeitung

Wenn zwei oder mehrere Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung festlegen, gelten sie gemäß Art. 26 Abs. 1 DSGVO als gemeinsam Verantwortliche. Entscheidend ist hierbei das Wesensmerkmal der Verantwortlichkeit: Jede beteiligte Stelle entscheidet sowohl über die Zwecke als auch über die Mittel der Verarbeitung.

Der EuGH hat in seiner Rechtsprechung (u. a. C 683/21) klargestellt, dass für eine gemeinsame Verantwortlichkeit jede der beteiligten Stellen eigenständig der Definition des »Verantwortlichen« nach Art. 4 Nr. 7 DSGVO entsprechen muss. Bezüglich des Ausmaßes des Einflusses der einzelnen Stellen betonte der EuGH (C 210/16, C 25/17, C 683/21), dass die Verantwortlichkeit nicht zwangsläufig gleichwertig sein muss. Vielmehr kann ein unterschiedlicher Grad der Verantwortlichkeit bestehen, der einzelfallbezogen danach bemessen wird, in welchen Phasen und in welchem Umfang die jeweiligen Beteiligten in die Verarbeitung einbezogen sind.

Gemeinsam Verantwortliche sind grundsätzlich verpflichtet, in einer Vereinbarung festzulegen, wer welche Pflichten aus der DSGVO übernimmt.

Abgrenzung zur Auftragsverarbeitung:

Im Gegensatz zur Auftragsverarbeitung ist bei der gemeinsamen Verantwortlichkeit jede beteiligte Stelle nicht weisungsgebunden, sondern trifft eigene Entscheidungen über Zwecke und Mittel der Datenverarbeitung. Bei der Auftragsverarbeitung hingegen handelt der Dienstleister ausschließlich nach Weisung des Verantwortlichen und verfolgt keine eigenen Zwecke.

[22] Petri/Stief in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Auflage 2025, DS-GVO Art.26 Gemeinsam Verantwortliche, Rn. 15-22.

Beispiele für gemeinsame Verantwortlichkeit:

- Zwei Unternehmen entwickeln gemeinsam eine Plattform für Online-Kundendaten und entscheiden gemeinsam über die Datenverarbeitungsprozesse und -zwecke. (Plattformbetrieb in Kooperation)
- Ein Verlag und ein Marketingdienstleister legen zusammen fest, wie Nutzerdaten für personalisierte Werbekampagnen verarbeitet werden.
- Shared Service innerhalb einer Unternehmensgruppe: Unternehmen A übernimmt die Personalverwaltung für Unternehmen B. Beide legen gemeinsam den Zweck (Personalverwaltung) und die Mittel (gemeinsame Personalsoftware) fest. Hier greift in der Regel die gemeinsame Verantwortlichkeit, da ein gemeinsames Interesse an der Verarbeitung besteht.

2.5 Wartung und Support

Wartungs- und Supportdienstleistungen an IT-Systemen stellen in der Regel keine Auftragsverarbeitung dar – vorausgesetzt, die Leistung zielt nicht auf eine gezielte Verarbeitung personenbezogener Daten ab, sondern beschränkt sich auf rein technischen Support, wie z. B. bei der Zugriffsgewährung zur Fehleranalyse und -behebung.

Dabei lässt sich nicht ausschließen, dass IT-Dienstleister gelegentlich Einsicht in personenbezogene Daten erhalten, etwa in Logfiles, Fehlermeldungen oder Systemdaten. Ein solcher bloßer Kenntnisnahme-Zugriff, der nicht planmäßig erfolgt, erfüllt jedoch nicht die Voraussetzungen einer Auftragsverarbeitung im Sinne des Art. 4 Nr. 8 DS-GVO. In diesen Fällen ist keine Vereinbarung nach Art. 28 DS-GVO erforderlich. Stattdessen ist der Anforderer gemäß Art. 24 DS-GVO verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um auch bei Support- und Wartungsarbeiten ein angemessenes Datenschutzniveau sicherzustellen. Zur Absicherung sollte vertraglich eine Verschwiegenheitsverpflichtung vereinbart werden. Dadurch wird dem Umstand Rechnung getragen, dass eine gelegentliche Einsichtnahme in personenbezogene Daten nicht ausgeschlossen werden kann, ohne dass eine planmäßige Verarbeitung stattfindet.

Abgrenzungskriterium: Planmäßigkeit der Datenverarbeitung

Eine Auftragsverarbeitung liegt nur dann vor, wenn der Dienstleister im Rahmen des Vertragsverhältnisses personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen verarbeitet. Nicht umfasst sind Leistungen, bei denen ein Zugriff auf personenbezogene Daten lediglich zufällig oder aus technischen Gründen erfolgen kann, ohne dass dies Ziel oder Gegenstand der Dienstleistung ist.

Typische Tätigkeiten der ITK-Branche, bei denen – sofern keine planmäßige Verarbeitung personenbezogener Daten erfolgt – keine Auftragsverarbeitung vorliegt, sind beispielsweise:

- Installation und Wartung von Netzwerken und Hardware (einschließlich TK-Anlagen)
- Pflege von Betriebssystemen, Middleware und Anwendungssoftware
- Parametrierung oder Konfiguration von Software
- Entwicklung, Anpassung oder Test von Programmen
- Fehlersuche und Supportmaßnahmen im Rahmen des Incident Managements

Auch in diesen Fällen können personenbezogene Daten innerhalb der Systeme des Anforderers verbleiben, ohne dass sie vom Dienstleister verarbeitet oder herausgegeben werden. Entscheidend ist, dass der Dienstleister nicht eigenständig über Zweck oder Mittel der Datenverarbeitung bestimmt, sondern lediglich technischen Support leistet.

Grenzfälle und Entwicklung zur Auftragsverarbeitung

Wichtig ist, dass die Dienstleistung im vereinbarten Rahmen bleibt (z. B. Support, Fehlerbehebung). Entwickelt sich der Leistungsumfang jedoch so, dass der Dienstleister regelmäßig personenbezogene Daten im Auftrag verarbeitet, ist rechtzeitig eine Vereinbarung gemäß Art. 28 DS-GVO zu schließen.

Hinweis für die Praxis:

Vor der Entscheidung über eine Vereinbarung nach Art. 28 DS-GVO sollte stets geprüft werden:

- Ist die Verarbeitung personenbezogener Daten zentraler Bestandteil der beauftragten Leistung?
- Verarbeitet der Dienstleister personenbezogene Daten regelmäßig, planmäßig und auf Weisung?
- Werden personenbezogene Daten außerhalb der Systeme des Auftraggebers verarbeitet oder übertragen?

Wenn alle Fragen verneint werden können, liegt in der Regel keine Auftragsverarbeitung vor. Dennoch sollten Vertraulichkeit und Datenschutz vertraglich geregelt werden.

3 Erläuterungen zu den Regelungen der Anlage

Das Muster ist im Einzelfall aufgabenspezifisch anzupassen. Soweit spezialgesetzliche Regelungen für die Daten, die im Auftrag verarbeitet werden, Anwendung finden, ist zunächst zu prüfen, ob eine Auftragsverarbeitung zulässig ist. Ggf. sind die spezialgesetzlichen Regelungen bei der Vertragsgestaltung (z. B. Beihilfe,- Personal-, Sozial- und Gesundheitsdaten) zu berücksichtigen.

Diese Mustervertragsanlage und die zugehörigen Erläuterungen orientieren sich an den Anforderungen des Art. 28 Abs. 3 DS-GVO. Bitte prüfen Sie zusätzlich, ob in Ihrem Anwendungsbereich besondere gesetzliche Regelungen gelten, die über die Vorgaben der DS-GVO hinausgehen.

Beispielhaft zu nennen sind etwa § 80 SGB X für die Verarbeitung von Sozialdaten sowie bestimmte Landesdatenschutzgesetze. Diese Vorschriften können zusätzliche Anforderungen enthalten, wie etwa:

- eine Anzeigepflicht des Auftraggebers gegenüber der zuständigen Aufsichtsbehörde bei der Beauftragung von Auftragsverarbeitern,
- oder ein weitergehendes Weisungsrecht des Auftraggebers, das sich auch auf die TOM erstreckt – im Unterschied zur DS-GVO, die dies in dieser Form nicht ausdrücklich vorsieht.

In solchen Fällen ist sicherzustellen, dass die spezifischen nationalen bzw. sektorspezifischen Anforderungen bei der Ausgestaltung der Auftragsverarbeitung berücksichtigt werden.

Anwendungsbereich

Die Anlage kann im Zusammenhang mit allen Verträgen Verwendung finden, die innerhalb Deutschlands oder zwischen einem deutschen Unternehmen und einem Unternehmen der Mitgliedsstaaten der Europäischen Union bzw. des Europäischen Wirtschaftsraums geschlossen werden. Bei einer Datenübermittlung in ein sog. Drittland muss jedoch ein angemessenes Datenschutzniveau sichergestellt sein.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Diese Klausel legt die grundsätzlichen Rahmenbedingungen der Auftragsverarbeitung im Sinne von Art. 28 Abs. 3 DSGVO fest.

Sie verweist auf Anlage 1 sowie gegebenenfalls auf den Hauptvertrag oder eine gesonderte Leistungsbeschreibung, aus denen sich die Art, der Zweck, der Umfang der Verarbeitung sowie die Kategorien betroffener Personen und Datenarten ergeben. Damit wird klargestellt, welche konkreten Datenverarbeitungsvorgänge vom Auftrag erfasst sind und zu welchen Zwecken sie stattfinden dürfen.

Das Muster geht in § 1 von einem Gleichlauf von Hauptvertrag und Auftragsverarbeitungsvertrag aus, das heißt: Die Laufzeit der Auftragsverarbeitung richtet sich grundsätzlich nach der Laufzeit des Hauptvertrags.

Abweichungen sind jedoch zulässig, insbesondere wenn datenschutzrechtliche Verpflichtungen (z. B. Lösch- oder Nachweispflichten) über das Vertragsende hinaus bestehen. Auch Auftragsverarbeitungsverträge mit unbefristeter Laufzeit sind grundsätzlich möglich, sofern eine Kündigungsmöglichkeit vorgesehen ist.

§ 2 Anwendungsbereich und Verantwortlichkeit

Diese Klausel konkretisiert die Rollen und Pflichten von Auftraggeber und Auftragnehmer im Sinne der Art. 4 Nr. 7 und 8, Art. 28 und Art. 29 DS-GVO.

Der Verantwortliche Auftraggeber (Art. 4 Nr. 7 DS-GVO)

- Trägt die Gesamtverantwortung für die Rechtmäßigkeit der Verarbeitung, auch wenn sie durch einen Dienstleister erfolgt.
- Muss prüfen, ob der AV-Dienstleister hinreichende Garantien bietet (Art. 28 Abs. 1 DS-GVO).
- Ist verpflichtet, einen schriftlichen oder elektronischen AV-Vertrag zu schließen (Art. 28 Abs. 3 DS-GVO).
- Darf und kann Kontrollrechte ausüben (z. B. Audits, Nachweise anfordern).

Der Auftragnehmer (Art. 4 Nr. 8 DS-GVO)

- Verarbeitet Daten ausschließlich auf dokumentierte Weisung (Art. 29 DS-GVO).
- Darf Unterauftragsverarbeiter nur mit Genehmigung des Verantwortlichen einsetzen (Art. 28 Abs. 2–4 DS-GVO).
- Muss technische und organisatorische Maßnahmen (TOMs) nach Art. 32 DS-GVO umsetzen.
- Unterliegt eigener Haftung, wenn er gegen Pflichten aus der DS-GVO verstößt (Art. 82 Abs. 2 DS-GVO)

Bereich	Verantwortlichkeit	Rechtsgrundlage
Prüfung, ob AV vorliegt	Verantwortlicher	Art. 4 Nr. 7, Art. 28 Abs. 1
Vertragsschluss & Kontrolle	Verantwortlicher	Art. 28 Abs. 3–6
Umsetzung der Weisungen, TOMs	Auftragsverarbeiter	Art. 28 Abs. 3 lit. c, f
Haftung bei Verstoß	Beide Seiten möglich	Art. 82 DS-GVO

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer muss den Weisungen des Auftraggebers folgen. Verstößt er gegen diese Pflicht der weisungsgebundenen Verarbeitung, indem er die Daten des Auftraggebers für eigene Zwecke oder Zwecke Dritter verarbeitet, wird er nach Art. 28 Abs.10 DS-GVO selbst zum Verantwortlichen mit allen rechtlichen Folgen z. B. auch zur Erfüllung der Betroffenenrechte. Art. 28 Abs. 10 DS-GVO benennt Ausnahmen a.G. rechtlicher Verpflichtungen, allerdings mit einer Informationspflicht hierüber an den Auftraggeber. Zur Art der Erteilung von Weisungen und der Nachweispflicht siehe vor (§ 2 Abs. 2)

(2) Da der Auftragnehmer für seine Ausführung der Weisungen gegenüber dem Auftraggeber nachweispflichtig ist, kann sich ein Problem ergeben, wenn er Weisungen erhält, die aus seiner Sicht rechtswidrig sind. Deshalb erlaubt Art. 28 Abs. 3 S. 3 DS-GVO ihm, solche Weisungen auszusetzen und seine Auffassung dem Auftraggeber mitzuteilen, der eine entsprechende Prüfung veranlasst. Im Ergebnis wird der Auftraggeber dem Auftragnehmer mitteilen, dass entweder die ursprüngliche Weisung bestätigt, oder aber entsprechend abgeändert – vielleicht sogar ganz ausgesetzt wird.

(3) Die Unterstützungspflicht des Auftragnehmers in Art. 28 Abs. 3 lit. e) DS-GVO gibt ihm ein Werkzeug an die Hand: technische und organisatorische Maßnahmen (TOM). Genauere Definitionen, welchem Zweck diese TOM dienen, finden sich in Art. 32 DS-GVO, auf den Art. 28 Abs. 3 lit. c) DS-GVO im Zusammenhang mit der Auftragsverarbeitung verweist. [Unabhängig davon hat der Auftraggeber selbst geeignete TOM für seine Verarbeitungen zu treffen (vgl. Art. 24 und Art. 25 DS-GVO, sowie ebenfalls Art. 32 DS-GVO)]. Dabei ist es unerheblich, ob die genannten Ziele – auch bekannt als IT-Ziele z.B. aus dem ISO 27.000-Bereich – mit zumeist unüberwindbaren technischen Maßnahmen – wie: Systemeinstellungen, Programme, konfigurierte Hardware, etc. – oder mit eher »weichen« organisatorischen Maßnahmen – wie: Richtlinien, Arbeitsanweisungen, Betriebs- bzw. Dienstvereinbarungen, etc. – bestehen, solange diese nachweisbar vorliegen und vom Auftragnehmer regelmäßig auf Einhaltung und Wirksamkeit überprüft werden.

Technische und organisatorische Maßnahmen stellen für die Verarbeitungsaufgaben beider Vertragsparteien entscheidende Mittel dar, um die Schutzziele der DS-GVO zu erreichen. Die vom Auftragnehmer getroffenen TOM stellt dieser dem Auftraggeber vor. Dies dient bereits vor Beginn der Verarbeitung dem Auftraggeber, sich zu versichern, dass er einen guten Vertragspartner gewählt hat (Art. 28 Abs. 1 DS-GVO; auch wenn es eine ausgesprochene Vorab-Prüfpflicht nicht (mehr) gibt). Zugleich kann der Auftraggeber sich bei seinen regelmäßigen Prüfungen (vgl. Art. 28 Abs. 3 lit. h) DS-GVO) darauf stützen und sich von der Einhaltung dieser TOM überzeugen.

Die Technik entwickelt sich weiter, somit sollen auch die TOM des Auftragnehmers sich weiter entwickeln und regelmäßig – im hier aufgeführten Rahmen und unter Beachtung des für die verarbeiteten Datenarten, Personengruppen, etc. erforderlichen Schutzniveaus – angepasst werden. Dabei bedeutet »Stand der Technik« in der »drei-Stufen-Theorie« (Bundesverfassungsgericht 1978; Kalkar-Entscheidung; Az. 2 BvL 8/77) sowohl für die allgemeine Anerkennung als auch für die Bewährung in der Praxis die mittlere Stufe, also unterhalb des »Stand der Wissenschaft und Forschung« der akademisch-wissenschaftlichen Erkenntnisse, aber auch oberhalb der »allgemein anerkannten Regeln der Technik«, über deren Wirksamkeit und praktischen Anwendbarkeit nicht diskutiert werden muss. Also definiert der Stand der Technik jene Methoden, die am besten funktionieren bzw. sich am Markt durchgesetzt haben (vgl. auch EN 45020 Normung – Allgemeine Begriffe (ISO/IEC Guide 2:2004), Ziffer 1.4).

Zugleich ist hier bereits eine Risikobewertung der TOM hinsichtlich der »Eintrittswahrscheinlichkeit und Schwere möglicher Risiken« angesagt, wie sie uns auch im Art. 35 DS-GVO begegnet. Im Idealfall können gleiche oder zumindest ähnliche Prozesse eingesetzt werden (siehe Kurzpapier 18 der DSK).

Aufgrund der Aufgabe der regelmäßigen Anpassung der TOM hat es sich in der Praxis bewährt, diese als (austauschbare) Anlage zu der Vereinbarung zur Auftragsverarbeitung zu gestalten. Alternativ können die jeweils aktuellen TOM auch über einen Link auf der Webseite des Auftragsverarbeiters bereitgestellt werden.

(4) Einer der Zwecke, für die der Auftragnehmer seine TOM gestaltet (aus Art. 28 Abs. 3 lit. e) DS-GVO): Die Unterstützung des Auftraggebers »nach Möglichkeit«, seinen Pflichten in Bezug auf Betroffenenrechte und deren Bearbeitung bzw. Erfüllung zu unterstützen. Er ist also nicht verpflichtet, exklusiv zur Erfüllung dieser Unterstützung spezielle Prozesse zu gestalten oder gar Ressourcen bereitzustellen, sondern lediglich zu tun, was ihm ohne gesonderte Aufwände bereits möglich ist. Dabei ist zu beachten, dass die Pflichten aus Kapitel III der DS-GVO exklusiv den Verantwortlichen treffen, der Auftragnehmer einer Auftragsverarbeitung also in keiner gesetzlichen Pflicht zur aktiven Erfüllung steht, sehr wohl aber als vertragliche Pflicht im zugrundeliegenden (Haupt-) Vertrag vereinbart sein kann, wobei der Auftraggeber nicht von seiner Verantwortlichkeit (insbes. aus Art. 5 Abs. 2 und seiner vertraglichen Allgemeinpflicht zur Überprüfung des Auftragnehmers und seiner Tätigkeiten) entbunden ist und beachtet werden muss, dass der Auftragnehmer – angesichts der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen – auch in der Lage ist, diese Aufgabe vollständig und fristgerecht zu erfüllen.

(5) Weitere Unterstützungen des Auftragnehmers fordert Art. 28 Abs. 3 lit. f) DS-GVO zur Erfüllung von Verpflichtungen des Auftraggebers, wobei sich auch hierbei der Auftragnehmer nicht besonders zu bemühen hat, sondern lediglich beisteuert, was

ihm bekannt sein müsste. Der Auftragnehmer muss den Weisungen des Auftraggebers folgen. Verstößt er gegen diese Pflicht der weisungsgebundenen Verarbeitung, indem er die Daten des Auftraggebers für eigene Zwecke oder Zwecke Dritter verarbeitet, wird er nach Art. 28 Abs.10 DS-GVO selbst zum Verantwortlichen mit allen rechtlichen Folgen z. B. auch zur Erfüllung der Betroffenenrechte.

(5a) und auf Art. 29 DS-GVO für den ausschließlichen Weisungsbezug seiner Tätigkeit

(5b) Die speziellen Pflichten des Auftragnehmers gehen zurück auf die Anforderungen von Art. 28 Abs. 3 lit. b) DS-GVO für die Vertraulichkeitsverpflichtung. Sollte das verarbeitende Personal nicht bereits durch ein Gesetz zur Vertraulichkeit verpflichtet sein (vgl. § 203 StGB zum Privatgeheimnis von Berufsträgern, wie Ärzten, Anwälten, Notaren, Steuerberatern, etc., sowie ähnlich lautende Regelungen in z.B. § 43e BRAO (i.V.m §2 BORA), § 26a BNotO, § 39c PAO, § 62a StBerG und § 50a WPO), so hat der Auftragnehmer eine angemessene Verpflichtung zur Vertraulichkeit schriftlich vorzunehmen und zu dokumentieren (→ Nachweispflicht). Dabei kann auch sogleich eine Verpflichtung auf die vom Auftraggeber erteilten Weisungen erfolgen. In der Praxis hat es sich bewährt, zumindest in einer Anlage (Merkblatt) Auszüge der relevanten Gesetze und Verordnungen, sowie möglicherweise der zugehörigen Bußgeld- oder Strafvorschriften mit der Verpflichtung auszuhändigen. Eine Verpflichtung zu § 203 StGB ist nur dann angezeigt, wenn der Auftragsverarbeiter die entsprechenden geheimzuhaltenden Daten (Patientendaten, Klientendaten, etc.), nicht jedoch, wenn er »nur« die allgemeinen personenbezogenen Daten eines Arztes oder Anwalts verarbeitet.

(6) Eine Spezifizierung der Unterstützungspflichten aus Art. 28 Abs. 3 lit. f) DS-GVO (siehe vor) i.V.m. Art. 33 Abs. 2 DS-GVO betrifft den sog. ‚Datenschutzvorfall'. Tritt nämlich beim Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten nach der Definition aus Art. 4 Nr. 12 DS-GVO auf, oder wird dem Auftragnehmer eine solche Verletzung gewahr, sollte er – im Rahmen einer Unterstützung – dazu verpflichtet sein, dem Auftraggeber alle wichtigen Informationen zu melden, damit dieser entscheiden kann, ob Meldungen und weitere Tätigkeiten nach Art. 33f DS-GVO erforderlich sind. Die Meldepflicht besteht ausschließlich für den Auftraggeber. Gleichwohl sollte der Auftragnehmer alle ihm bekannten Informationen mitteilen, damit der Auftraggeber die nach Art. 33 Abs. 3 bzw. Abs. 34 Abs. 3 DS-GVO erforderlichen Meldungen absetzen kann. Es liegt in der Natur der Dinge, dass der Auftragnehmer nicht unbedingt alles weiß, was der Auftraggeber zu melden hat, doch was ihm bekannt ist, sollte er weitergeben. Die in Art. 33 Abs. 1 DS-GVO genannte Frist ‚möglichst binnen 72 Stunden' trifft den Auftragnehmer nicht, da diese Frist erst dann beginnt, wenn dem Auftraggeber der Vorfall bekannt wird. Gleichwohl sollte die Weitergabe der Informationen an den Auftraggeber nicht verzögert werden, da sich die Situation ohne dessen Eingreifen möglicherweise verschlechtern könnte. Es hat sich bewährt, dem Auftragnehmer vertraglich eine Frist zu setzen, zumeist binnen 24 Stunden. In der Praxis bewährt: Vorbereitete Fragebögen für die Beschäftigten des Auftragnehmers, als auch vorbereitete Meldebögen zur Information des Auftraggebers.

(7) Der Auftraggeber hat gelegentlich Bedarf, sich an eine mit dem Datenschutz vertraute Stelle beim Auftragnehmer zu wenden (das beruht auf Gegenseitigkeit, siehe § 4 Abs. 2). Dazu reicht eine »Kontaktinformation« – wie z.B. eine dafür geeignete E-Mail-Adresse – aus. Es ist nicht erforderlich, dass Namen und Anschriften genannt

werden, solange sichergestellt ist, dass über die genannte Information ein Kontakt ‚zügig' erfolgen kann, wenn dies notwendig ist. In der Praxis hat es sich bewährt, dazu ein Funktionspostfach einzurichten, auf welches der DSB (sofern bestellt) oder eine andere, fachkundige Person Zugriff hat. Bitte an Abwesenheitsregelungen während Krankheit, Urlaub, etc. denken, also für Belange der eigenen Beschäftigten des Auftragnehmers ein anderes Postfach verwenden (wg. Schweigepflicht des DSB). Mit Nutzung eines Funktionspostfachs entfällt eine Aktualisierungsmeldung an den Auftraggeber bei Wechsel der zuständigen Person, wie es im Falle eines namentlichen Kontaktes notwendig wäre – in diesen Fällen sollte eine Aktualisierungsmitteilung vertragliche Pflicht sein. In einer Meldung eines Datenschutzvorfalls (siehe vor) muss ebenfalls eine Kontaktinformation genannt werden, um eine schnelle Bearbeitung bei Nachfragen zu ermöglichen.

(8) Herausgabe oder Löschen ‚nach Abschluss der Erbringung der Verarbeitungsleistungen aller personenbezogenen Daten' wird von Art. 28 Abs. 3 lit. g) DS-GVO vorgegeben. Dabei inkludiert ‚Herausgabe' in der Praxis das anschließende Löschen, es sollen also keine Daten beim Auftragnehmer zurückbleiben, es sei denn dieser benötigt die Daten zur Erfüllung eigener Rechtspflichten. Durch falsche Interpretation der Vorgabe aus der DS-GVO zum Zeitablauf (‚nach' Abschluss) und der Tätigkeit (Erbringung der Verarbeitungsleistung) können sich Probleme für die beteiligten Parteien ergeben. So hat nach Vertragsende der Auftraggeber kein Weisungsrecht mehr und ohne Weisung darf der Auftragnehmer nicht verarbeiten, also auch nicht herausgeben und/oder löschen. Dem sollte begegnet werden, indem z.B. bei Kündigung des Vertrages bereits die Erfüllung des Wahlrechts durch den Auftragnehmer eingefordert wird. In der Praxis hat es sich bewährt, vertraglich bereits eine Weisung vorzusehen, falls der Auftraggeber nicht rechtzeitig von seinem Recht Gebrauch macht. Beispiel: »Macht der Auftraggeber nicht rechtzeitig vor Vertragsende von seinem Wahlrecht Gebrauch, so ist der Auftraggeber berechtigt, nach sechs Monaten die Auftraggeberdaten zu löschen.« Übrigens ist hiermit gesetzlich nicht geregelt, ob und wie oft der Auftraggeber ‚während der Erbringung der Verarbeitungsleistung' eine Herausgabe (eines Teils) der Daten verlangen darf. Da der Auftragnehmer also eine Leistung erbringen soll, erlaubt ihm das allgemeine Vertragsrecht, dies in Rechnung zu stellen, bzw. fairerweise vorab ein Angebot zu unterbreiten.

Opt: Grundsätzlich ist der Auftragnehmer immer berechtigt, die Erbringung einer Dienstleistung nach allgemeinem Vertragsrecht in Rechnung zu stellen. Der Auftraggeber kann jedoch davon ausgehen, dass bestimmte Leistungserbringungen bereits eingepreist sind, sofern Umfang und Häufigkeit der Leistungserbringung für den Auftragnehmer vorab einschätzbar waren und die Anforderung zur Leistungserbringung durch den Auftraggeber in Umfang und Häufigkeit nicht ungewöhnlich erfolgt. So muss der Auftragnehmer, wenn er bestehende Prozesse zur Löschung und/oder Herausgabe hat, anderslautende Vorgaben, wie die Überbringung der Daten per Kurier, nicht kostenneutral erbringen. Vielmehr sollte dem Auftraggeber ein Angebot zur kostenneutralen Erledigung der gesetzlichen Pflichten unterbreitet werden. Besteht dieser auf seiner Vorgabe, kann immer über die Teilung der Kosten verhandelt werden.

§ 4 Pflichten des Auftraggebers

Da in der DS-GVO auch spezielle Haftungsregelungen für den Auftragsverarbeiter bei Datenschutzverletzungen hinzugekommen sind, wonach der Betroffene direkt vom Auftragsverarbeiter Schadenersatz fordern kann, muss der Verantwortliche den Auftragsverarbeiter bei der Abwehr des Anspruchs unterstützen.

Laut LfD Niedersachsen liegt eine Auftragsverarbeitung dann vor wenn:

»Eine Auftragsverarbeitung liegt nur vor, wenn der Auftragnehmer Daten im Auftrag und nach Weisung des Auftraggebers verarbeitet. Sobald der Auftragnehmer eigene Zwecke verfolgt oder eigenverantwortlich handelt, ist keine Auftragsverarbeitung gegeben.«

Der Auftraggeber muss also vor Beginn jeder Zusammenarbeit prüfen, ob eine echte Auftragsverarbeitung vorliegt, um Art. 28 DS-GVO anzuwenden.

A. Anwendungsbereich der Auftragsverarbeitung für den Auftraggeber

1. Wann ist der Auftraggeber im Anwendungsbereich verantwortlich:

   Der Auftraggeber im Sinne des Art. 28 DS-GVO ist derjenige, der über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (Art. 4 Nr. 7 DS-GVO). Sobald dieser für die Datenverarbeitung einen externen Dienstleister einsetzt, der die Daten nicht für eigene Zwecke, sondern ausschließlich auf Weisung verarbeitet, liegt eine Auftragsverarbeitung vor.

2. Wann ist der Auftraggeber nicht im Anwendungsbereich verantwortlich:

   - der Dienstleister eigene Zwecke verfolgt (z. B. Steuerberater, Arzt, Anwalt, Auskunftei),
   - die Datenverarbeitung gesetzlich vorgegeben ist (z. B. Meldung an Behörden),
   - oder der Dritte faktisch nicht in den Verarbeitungsvorgang eingreift (z. B. Postdienstleister, reine Transportleistung).

B. Verantwortung des Auftraggebers

Der Auftraggeber (Verantwortliche) bleibt Herr der Daten. Auch dann, wenn ein Dienstleister die Verarbeitung übernimmt, trägt der Auftraggeber die datenschutzrechtliche Hauptverantwortung.

Tabelle: Pflichten des Auftraggebers nach Art. 28 DS-GVO

Pflicht	Beschreibung	Rechtsgrundlage
Prüfung der Zulässigkeit	Bevor Daten übermittelt werden, muss geprüft werden, ob die Verarbeitung rechtmäßig ist (Art. 6 DS-GVO).	Art. 5 Abs. 1 a), Art. 6
Auswahlpflicht	Nur Auftragsverarbeiter einsetzen, die hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (TOMs) bieten.	Art. 28 Abs. 1
Vertragspflicht	Abschluss eines schriftlichen oder elektronischen Vertrags mit allen Mindestinhalten des Art. 28 Abs. 3 DS-GVO.	Art. 28 Abs. 3
Weisungsrecht und Kontrolle	Der Auftraggeber muss Weisungen erteilen und darf die Einhaltung regelmäßig prüfen (Audits, Nachweise, Zertifikate).	Art. 28 Abs. 3 lit. a, h
Nachweispflicht	Verantwortlicher muss die Einhaltung der DS-GVO dokumentieren (Rechenschaftspflicht).	Art. 5 Abs. 2
Verzeichnis der Verarbeitungstätigkeiten	Auftragsverarbeitungen müssen im Verzeichnis nach Art. 30 DS-GVO geführt werden.	Art. 30 Abs. 1
Ende des Auftrags	Nach Abschluss: Löschung oder Rückgabe der Daten sicherstellen.	Art. 28 Abs. 3 lit. g

C. Umsetzung in der Praxis

Der Auftraggeber sollte für jede AV folgende Implementierungsschritte durchführen:

1. Prüfung des Anwendungsbereichs
   - Liegt Auftragsverarbeitung vor (Weisungsgebundenheit)?
   - Oder gemeinsame Verantwortlichkeit / eigener Zweck des Dienstleisters?
2. Due Diligence vor Vertragsschluss
   - Prüfen von TOMs, Zertifizierungen, Referenzen, IT-Sicherheitskonzept.
   - ggf. Datenschutz-Checkliste oder Selbstauskunft des Dienstleisters einholen.
3. Vertrag abschließen

Der AV-Vertrag muss u. a. regeln (vgl. Art. 28 Abs. 3 lit. a–h DS-GVO):

- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,
- Art der personenbezogenen Daten und Kategorien der betroffenen Personen,
- Pflichten und Rechte des Verantwortlichen,
- Pflichten des Auftragsverarbeiters (z. B. Weisungen, Vertraulichkeit, TOMs, Unteraufträge, Löschung).

4. Weisungsmanagement und Kontrolle
   - Regelmäßige Nachweise, Auditberichte oder Zertifikate anfordern.
   - Dokumentation der Weisungen und Ergebnisse der Prüfungen.
5. Auftragsende regeln
   - Sichere Rückgabe oder Löschung der Daten.
   - ggf. Übergabeprotokoll oder Löschbestätigung.

D. Typische Fehler des Auftraggebers

Fehler	Folge
Keine Prüfung, ob überhaupt AV vorliegt	Falsche Rechtsgrundlage / Bußgeldrisiko
Kein schriftlicher AV-Vertrag	Verstoß gegen Art. 28 → Bußgeld nach Art. 83 DS-GVO

Fehler	Folge
Fehlende Kontrolle des Dienstleisters	Verletzung der Rechenschaftspflicht
Unzureichende Dokumentation	Nachweismangel bei Datenschutzaufsicht
Fehlende Regelung zur Löschung	Risiko fortgesetzter Datenverarbeitung nach Auftragsende

E. Kurzfazit für den Auftraggeber:

Der Auftraggeber bleibt immer »Herr der Daten« – auch wenn die Verarbeitung technisch ausgelagert wird.

Aufgabe	Verantwortlich	Grundlage
Prüfung, ob AV vorliegt	Auftraggeber	Art. 28 Abs. 1
Auswahl und Kontrolle des Verarbeiters	Auftraggeber	Art. 28 Abs. 1–3
Vertragserstellung und -dokumentation	Auftraggeber	Art. 28 Abs. 3
Nachweis der Einhaltung (Accountability)	Auftraggeber	Art. 5 Abs. 2
Verantwortung für Rechtsgrundlage der Datenverarbeitung	Auftraggeber	Art. 6 DS-GVO

§ 5 Anfragen betroffener Personen

Die Person, deren personenbezogene Daten verarbeitet werden (sog. Betroffener), kann ihre Rechte (z. B. Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung, vgl. Kapitel III der DS-GVO) gegenüber dem Unternehmen bzw. der öffentlichen Stelle geltend machen, das bzw. die personenbezogene Daten des Betroffenen als Verantwortlicher verarbeitet. Bei einer Auftragsverarbeitung bleibt daher der Auftraggeber als Verantwortlicher Adressat dieser Ansprüche. Sollte sich ein Betroffener direkt an den Auftragsverarbeiter wenden, hat dieser die Betroffenen-

Anfrage unverzüglich an den Verantwortlichen weiterzuleiten. Es sollte ein Verfahren zwischen Auftraggeber und Auftragnehmer festgelegt werden, das sicherstellt, den Rechten des Betroffenen nachkommen zu können. Die Verantwortung hierfür und auch die entstehenden Kosten (z. B. durch einen Herausgabe- oder Löschungsanspruch von Daten) trägt der Auftraggeber als Verantwortlicher.

§ 6 Nachweismöglichkeiten

Damit der Auftraggeber seinerseits seiner Rechenschaftspflicht gemäß Art. 24 Abs. 1 i.V.m Art. 5 Abs. 2 DS-GVO nachkommen kann, ist eine lückenlose Dokumentation der Einhaltung der organisatorischen Maßnahmen notwendig.

§ 6 Abs. 5 verlangt hinsichtlich der Einhaltung der Maßnahmen daher "geeignete Mittel".

Zu diesen geeigneten Nachweismitteln zählen die in § 6 Abs. 2 aufgelisteten Möglichkeiten. Neben regelmäßigen Aufzeichnungen können hierzu auch systemseitig erzeugte Protokolle, Prüfberichte oder Audit-Logs gehören, die den datenschutzkonformen Betrieb dokumentieren. In der Praxis wird häufig auf Berichte unabhängiger Instanzen zurückgegriffen, etwa Wirtschaftsprüfer, interne Revision, externe Datenschutzauditoren oder Zertifizierungsstellen. Zertifikate nach anerkannten Standards (z. B. ISO 27001, ISO 27701, BSI C5) oder branchenspezifische Audits können regelmäßig als ausreichender Nachweis dienen, sofern sie aktuell sind und den relevanten Geltungsbereich der Verarbeitung abdecken.

Die DS-GVO enthält keine ausdrückliche Regelung dazu, in welchem Umfang der Auftraggeber die Verarbeitungstätigkeiten des Auftragnehmers überwachen muss. Artikel 28 Abs. 3 S. 2 lit. h DS-GVO verpflichtet den Auftragnehmer jedoch, dem Verantwortlichen Überprüfungen – einschließlich Inspektionen – zu ermöglichen. Um seiner Nachweispflicht gemäß Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO nachzukommen, muss der Auftraggeber also über vertraglich abgesicherte Kontrollrechte verfügen (§ 6 Abs. 3).

Die DS-GVO schreibt dabei keine bestimmte Form der Kontrolle vor. Neben Dokumentenprüfungen und technischen Nachweisen kommen auch Vor-Ort-Inspektionen in Betracht, die durch den Verantwortlichen selbst oder durch externe Prüfer durchgeführt werden können. Letztere sind in der Praxis oft sinnvoll, da es dem Auftraggeber häufig an technischem Know-how oder personellen Ressourcen für tiefgehende Audits fehlt.

§ 6 Abs. 3 lit. d Opt. 2 konkretisiert das Kontrollrecht, indem es eine reguläre Prüfung pro Kalenderjahr vorsieht. Ergänzend sollten anlassbezogene Kontrollen, etwa im Fall einer Datenschutzverletzung oder wesentlicher Systemänderungen, vertraglich vereinbart werden. Alternativ kann die Häufigkeit der Inspektionen auch allgemeiner gefasst werden (z. B. »regelmäßig« oder »in angemessenen Abständen«), um den Parteien mehr Flexibilität bei der praktischen Ausgestaltung der Kontrollen zu ermöglichen.

§ 7 weitere Auftragsverarbeiter (Unterauftragsverarbeiter)

§ 7 setzt Art. 28 Abs. 3 lit. d DSGVO um, wonach die Voraussetzungen und Bedingungen für die Einschaltung weiterer Auftragsverarbeiter im Auftragsverarbeitungsvertrag festzustellen ist

§ 7 Abs. 1 sieht vor, dass eine Liste der Subunternehmer, die in der Anlage xxx steht, als genehmigt vom Auftraggeber anzusehen ist. Diese Regelung schafft Transparenz und dokumentiert zugleich, dass die dort genannten Unternehmen bereits einer datenschutzrechtlichen Prüfung durch den Auftraggeber unterzogen wurden oder im Rahmen der Vertragsverhandlungen als vertrauenswürdig eingestuft worden sind.

§ 7 Abs. 2 regelt die Voraussetzungen für die Beauftragung weiterer Auftragsverarbeiter, sofern diese nicht in der Liste der genehmigten Subunternehmer enthalten sind.

§ 7 Abs. 2

Variante 1 sieht entsprechend Art. 28 Abs. 2 DS-GVO die Möglichkeit einer Einzelfallgenehmigung vor, wobei der Begriff der »Genehmigung« in diesem Zusammenhang autonom im Sinne einer vorherigen ausdrücklichen Zustimmung gemäß § 183 BGB auszulegen ist.

Variante 2 beschreibt dagegen die sog. »allgemeine Genehmigung«: Sie erlaubt dem Auftragnehmer, neue Subunternehmer einzusetzen, sofern der Auftraggeber rechtzeitig – in der Regel mindestens 14 Kalendertage vorher – informiert wird und innerhalb dieser Frist kein Widerspruch erfolgt. Dieses Modell wird in der Praxis häufig bevorzugt, da es einen flexibleren Umgang mit Änderungen in der Dienstleisterstruktur ermöglicht, ohne den Auftraggeber seiner Kontrollrechte zu berauben. Die Frist von 14 Tagen hat sich in vielen Standardverträgen als angemessen etabliert.

Zu beachten ist, dass die allgemeine Genehmigung nur wirksam ist, wenn sie mit einem echten Widerspruchsrecht verbunden ist – fehlt dieses, liegt keine hinreichende Kontrolle des Auftraggebers mehr vor (vgl. Erwägungsgrund 81 DS-GVO).

Gemäß § 7 Abs. 3 stellt der Auftragnehmer dem Auftraggeber eine aktuelle Liste aller eingesetzten Subunternehmer zur Verfügung. Diese Liste wird als Anlage zum Vertrag beigefügt oder alternativ über einen eindeutig benannten, dauerhaft zugänglichen Internet-Link bereitgestellt.

Dabei sollten Identität, Tätigkeitsumfang und Verantwortungsbereich des jeweiligen Unterauftragnehmers klar beschrieben werden. Hierzu zählen insbesondere die von ihm zu erbringenden Leistungen, der Zweck der Datenverarbeitung, die Kategorien der

verarbeiteten Daten sowie der Kreis der betroffenen Personen. Eine solche Spezifizierung ist insbesondere deshalb ratsam, weil Unterauftragnehmer in der Regel nur Teilaufgaben übernehmen und daher eine eindeutige Abgrenzung der Tätigkeitsbereiche erforderlich ist.

Diese Angaben ermöglichen es dem Auftraggeber, zu prüfen, ob der Einsatz des jeweiligen Subunternehmers mit den Anforderungen der DS-GVO im Einklang steht – insbesondere im Hinblick auf etwaige Datenübermittlungen in Drittländer (Art. 44 ff. DS-GVO) oder Verarbeitungen außerhalb des EWR. In der Praxis hat es sich bewährt, die Liste regelmäßig – mindestens einmal jährlich oder nach jeder Änderung – zu aktualisieren und dem Auftraggeber proaktiv zur Verfügung zu stellen.

§ 7 Abs. 4 sieht eine Spiegelung der Regelungen des übergeordneten Auftragsverarbeitungsvertrages auf den Subunternehmervertrag vor (Art. 28 Abs. 4 DS-GVO). Das bedeutet, dass der Auftragnehmer seine Pflichten aus dem Hauptvertrag vollständig an den Subunternehmer weitergeben muss. In der Praxis empfiehlt es sich, Muster-AV-Verträge oder Standardklauseln zu verwenden, um ein einheitliches Datenschutzniveau sicherzustellen.

Das vorliegende Muster geht von einer vollständigen Weiterleitung der Verarbeitung der Auftraggeberdaten an den Unterauftragsnehmer aus. Sofern nur einzelne Teile der Datenverarbeitung weitergereicht werden, muss an dieser Stelle eine sachbereichsspezifische Anpassung vorgenommen werden.

Hinweis: Wichtig ist klarzustellen, dass der Genehmigungsvorbehalt nicht für sämtliche Vertragsverhältnisse gilt, sondern nur für solche, bei denen ein Zugriff auf personenbezogene Daten des Auftraggebers nicht ausgeschlossen werden kann. Dies hat den Hintergrund, dass in der Praxis oft Unklarheit darüber herrscht, ob es sich um eine Unterbeauftragung im datenschutzrechtlichen Sinne handelt. Nicht erfasst sind daher Vertragsverhältnisse, denen reine Nebenleistungen zugrunde liegen, die keinen konkreten Bezug zu den im Auftrag erbrachten Leistungen haben, z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Bewachungsdienste oder Telekommunikationsleistungen. Für diese ist keine Genehmigung erforderlich, sofern ein Zugriff auf personenbezogene Daten ausgeschlossen ist.
(Siehe auch Kap. 2.1 dazu)

§ 8 Übermittlung in Drittstaaten

Laut § 8 Abs. 1 ist eine Übermittlung außerhalb des Gebiets der EU und des EWR von einer dokumentierten Weisung des Verantwortlichen und der Beachtung der Voraussetzungen der Art. 44 ff. DS-GVO abhängig.

Wie in § 8 Abs. 2 beschrieben, regelt Art. 45 DS-GVO eine Datenübermittlung für die Fälle, in denen ein Angemessenheitsbeschluss der EU-Kommission vorliegt. Liegt ein solcher Beschluss nicht vor, kommt eine Übermittlung personenbezogener Daten nur auf Grundlage geeigneter Garantien gemäß Art. 46 DS-GVO in Betracht, sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

Zu den geeigneten Garantien zählen insbesondere:

- Standarddatenschutzklauseln der EU-Kommission (Art. 46 Abs. 2 lit. c, d DS-GVO),
- verbindliche interne Datenschutzvorschriften (»Binding Corporate Rules«, Art. 47 DS-GVO),
- genehmigte Verhaltensregeln oder Zertifizierungsmechanismen (Art. 46 Abs. 2 lit. e, f DS-GVO).

Nach § 8 Abs. 2 verpflichtet sich der Auftragnehmer zudem, bei Verwendung von Standardvertragsklauseln ein sogenanntes Transfer Impact Assessment (TIA) durchzuführen. Dieses dient der Bewertung, ob im Empfängerland ein der EU gleichwertiges Schutzniveau gewährleistet ist, und ob ggf. zusätzliche technische, organisatorische oder vertragliche Maßnahmen erforderlich sind. Das TIA ist zu dokumentieren und dem Auftraggeber auf Anfrage bereitzustellen.

Hinweis: Datenübermittlung in die USA (Data Privacy Framework)

Am 10. Juli 2023 hat die Europäische Kommission den Angemessenheitsbeschluss für den Datenschutzrahmen EU–USA (Data Privacy Framework, DPF) erlassen. Danach dürfen personenbezogene Daten nur an nach dem DPF zertifizierte US-Unternehmen übermittelt werden. Datenübermittlungen an nicht zertifizierte Unternehmen können nicht auf den Angemessenheitsbeschluss gestützt werden und erfordern weiterhin geeignete Garantien (siehe § 8 Abs.2).

§ 8 Abs. 3 stellt klar, dass eine Drittlandsverarbeitung durch den Auftragnehmer oder dessen Subunternehmer nur mit vorheriger Zustimmung des Auftraggebers zulässig ist, sofern nichts anderes vereinbart wurde. Dadurch wird sichergestellt, dass der Auftraggeber die Kontrolle über etwaige Datenübermittlungen außerhalb des EWR behält.

Hinweis: Insbesondere vor der Inanspruchnahme von Cloud-Dienstleistungen ist daher sorgfältig zu prüfen, ob die Datenverarbeitung eine Übermittlung in ein Drittland einschließt und ob die Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Es empfiehlt sich zudem, im Vertrag klarzustellen, ob Cloud-Anbieter (z. B. US-Unternehmen mit EU-Servern) als Subunternehmer nach § 7 einzustufen sind und ob ein entsprechender Genehmigungsvorbehalt greift.

§ 9 Haftung

§ 9 verweist auf das Haftungsregime der DS-GVO sowie gegebenenfalls auf Regelungen im Hauptvertrag. Grundprinzip: Jede betroffene Person, die durch einen Verstoß gegen die DS-GVO materiellen oder immateriellen Schaden erleidet, kann Schadenersatzansprüche geltend machen – entweder gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

- **Haftung des Auftragsverarbeiters (Art. 82 Abs. 2 S. 2 DS-GVO)**: Der Auftragsverarbeiter haftet nur, wenn er Pflichten aus dem Vertrag oder der DS-GVO verletzt oder weisungswidrig gehandelt hat.
- **Gesamtschuldnerische Haftung (Art. 82 Abs. 4 DS-GVO)**: Verantwortlicher und Auftragsverarbeiter haften gemeinsam gegenüber der betroffenen Person.
- **Interner Ausgleich (Art. 82 Abs. 5 DS-GVO)**: Für den Ausgleich innerhalb der Schuldnergemeinschaft gilt die Haftung nach tatsächlichem Verursachungsbeitrag, vorrangig vor § 426 BGB.

Exkulpationsmöglichkeit (Art. 82 Abs. 3 DS-GVO): Verantwortlicher oder Auftragsverarbeiter können nachweisen, dass sie in keinerlei Hinsicht für den Schaden verantwortlich sind, um sich von der Haftung zu befreien.

§ 10 Informationspflichten, Schriftformklausel, Rechtswahl

Informationspflicht: Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn die Daten gefährdet sind, z. B. durch Pfändung, Beschlagnahme oder Insolvenz.

Schriftform: Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform, die auch elektronisch (Textform, § 126b BGB) erfolgen kann. Dies gilt ausdrücklich auch für den Verzicht auf das Formerfordernis.

Hinweis: In AGB kann eine solche Klausel unwirksam sein, wenn sie den Eindruck erweckt, mündliche Nachverhandlungen seien generell ausgeschlossen (§ 305b BGB). Praktisch empfiehlt es sich daher, die Textform zuzulassen.

Salvatorische Klausel: Sollten einzelne Teile der Vereinbarung unwirksam sein, bleibt die Vereinbarung im Übrigen wirksam (Erhaltungsfunktion, § 306 Abs. 1 BGB).

Vorrang: Bestimmungen dieser Vereinbarung haben Vorrang vor Regelungen des Hauptvertrages.

Rechtswahl: Es gilt deutsches Recht.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Ansprechpartner/in

Elena Kouremenou | Referentin Datenschutz

T +49 30 27576-425 | e.kouremenou@bitkom.org

Verantwortliches Bitkom-Gremium

AK Datenschutz

Autorinnen und Autoren

Joy Achilles | Datev eG

Dr. Alexander Fritz | OmegaLambdaTec GmbH – Data Science Services

Nicolas Garea | Daten eG

Mühlhaus Thorsten | P&I Personal & Informatik AG

Hannah Seiffert | Computacenter AG & Co. oHG

Kathrin Steffens |]init[AG für digitale Kommunikation

Zur ursprünglichen Version des Leitfadens hatten maßgeblich beigetragen: Joseph Beck, Mareike Böddeker, Sebastian Brüggemann, Giovanni Brugugnone, Almuth Flunkert, Markus Frowein, Hens Gehrandt, Wulf Kamlah, Rudi Kramer, Illona Lindemann, Regina Mühlich, Karolina Rozek, Martin Schweinoch, Sylle Schreyer-Bestmann, Andreas Splittgerber, Hendrik Tamm, Florian Thoma, Christian Wagner, Stephan Weinert