Die Landesbeauftragte für den
Datenschutz Niedersachsen

FAQ zur Auftragsverarbeitung nach Artikel 28 der Datenschutz-Grundverordnung

Stand: August 2022

Inhaltsverzeichnis

1. Was versteht man unter einer Auftragsverarbeitung?

Bei der Auftragsverarbeitung handelt es sich um eine spezifische Form der Aufgabenübertragung bei der Verarbeitung personenbezogener Daten.

Der Verantwortliche (im Sinne der Definition des Artikels 4 Nummer 7 DS-GVO) lagert dabei in der Regel Teilprozesse, die er sonst selbst vornehmen müsste und bei denen personenbezogene Daten verarbeitet werden, an einen externen Dienstleister (= Auftragsverarbeiter im Sinne der Definition des Artikels 4 Nummer 8 DS-GVO) aus („Outsourcing“).

Beispiel:

Ein Unternehmen übernimmt im Auftrage des Verantwortlichen die datenschutzkonforme Vernichtung von Dokumenten oder Datenträgern.

2. Wann ist die beauftragte Verarbeitung personenbezogener Daten eine Auftragsverarbeitung nach Artikel 28 Absatz 1 DS-GVO?

Eine Auftragsverarbeitung nach Artikel 28 Absatz 1 DS-GVO liegt vor, wenn die beiden folgenden Fragen mit „Ja“ beantwortet werden können.

2.1 Werden bei dem Verarbeitungsprozess personenbezogene Daten verarbeitet?

Personenbezogene Daten sind zum Beispiel Informationen über

- Kunden und
- Beschäftigte.

Hierzu zählen insbesondere

- Name, Alter, Familienstand, Geburtsdatum,
- Kontaktdaten, wie postalische Anschrift, Telefonnummer, E-Mail-Adresse, umfasst sind hier auch dienstliche Kontaktdaten, soweit sie einen Personenbezug aufweisen, wie max.mustermann@unternehmen.de oder die persönliche dienstliche Durchwahl,
- Bankverbindungsdaten, wie Konto- oder Kreditkartennummer,
- Kraftfahrzeugnummer, Kfz-Kennzeichen,
- Personalausweis- und Sozialversicherungsdaten, einschließlich der Ausweis- und Versicherungsnummern sowie
- genetische Daten und Gesundheitsdaten.

Dabei ist die technische Form dieser Angaben nicht von Bedeutung. Auch Fotos, Videoaufnahmen, Röntgenbilder oder Tonbandaufnahmen können personenbezogene Daten enthalten.

2.2 Erfolgt die Verarbeitung personenbezogener Daten nicht durch den Verantwortlichen selbst, sondern durch einen speziell mit dieser Datenverarbeitung beauftragten Dienstleister?

Eine Auftragsverarbeitung im Sinne des Artikel 28 DS-GVO liegt grundsätzlich dann vor, wenn ein Dienstleister nach einem Auftrag und konkreten Vorgaben des datenschutzrechtlich Verantwortlichen eine Datenverarbeitung vornimmt. Der Dienstleister entscheidet dabei nicht selbst über die wesentlichen Umstände der Datenverarbeitung und hat kein eigenes, über die Erfüllung des Auftrags hinausgehendes, Interesse an der Datenverarbeitung. Eine Auftragsverarbeitung ist folglich regelmäßig bei den folgenden Dienstleistungen anzunehmen:

- Entsorgung (Vernichtung, Löschung) von Datenträgern mit personenbezogenen Daten durch Dienstleister,
- Speicherung von personenbezogenen Daten in der Cloud,
- Werbeadressenverarbeitung in einem Letter-Shop,
- Verarbeitung von Kundendaten durch ein Call-Center ohne wesentliche eigene Entscheidungsspielräume dort,
- Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten mit personenbezogenen Daten,
- DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren,
- elektronische Rechnungserstellung[1].

3. Ist für die vom Auftragsverarbeiter vorgenommene Verarbeitung personenbezogener Daten eine Rechtsgrundlage erforderlich?

Ja. Allerdings benötigt der Auftragsverarbeiter keine „eigene“ Rechtsgrundlage. Stattdessen stützt er sich für die Verarbeitung personenbezogener Daten „im Auftrag“ auf die dem Verantwortlichen zustehende datenschutzrechtliche Rechtsgrundlage. Der Auftragsverarbeiter wird nicht als Dritter (Artikel 4 Nummer 10 DS-GVO) angesehen, sondern „als verlängerter Arm“ des Verantwortlichen.

[1] Für Leistungserbringende im Gesundheitswesen sind in diesem Zusammenhang berufsrechtliche Voraussetzungen zu beachten. Insbesondere greift in diesen Fällen das Privileg der Auftragsverarbeitung nicht vollumfänglich; vielmehr ist eine nachweisbare Einwilligung der Patienten erforderlich (vergleiche zum Beispiel § 12 Absatz 2 der Berufsordnung der Ärztekammer Niedersachsen).

Eine eigene Rechtsgrundlage für die Verarbeitung im Auftrag ist jedoch nur dann entbehrlich, wenn

- die beauftragte Verarbeitung personenbezogener Daten tatsächlich eine Auftragsverarbeitung nach Artikel 28 Absatz 1 DS-GVO ist (siehe Frage 2),
- der Auftragsverarbeiter ausschließlich gemäß dem Auftrag weisungsgebunden handelt (Artikel 29 DS-GVO) und
- eine jederzeitige Kontrolle des Verantwortlichen bzgl. der Einhaltung der Pflichten durch den Auftragsverarbeiter ermöglicht wird (Artikel 28 Absatz 3 Buchstabe h DS-GVO).

Trotz der Auslagerung von Aufgaben an den Dienstleister bleibt der Verantwortliche für die Datenverarbeitung nach außen, also Betroffenen und Dritten gegenüber, in vollem Umfang verantwortlich.

In Bezug auf die Privilegierung kann sich allenfalls etwas anderes ergeben, wenn

- eine Datenverarbeitung keine Auftragsverarbeitung nach Artikel 28 DS-GVO ist oder
- sich der Auftragsverarbeiter vertragswidrig verhalten sollte, indem er
    - sich nicht an die Weisungen des Verantwortlichen hält oder
    - die Auftragsdaten für eigene Zwecke nutzt (siehe Artikel 28 Absatz 10 DS-GVO). Inhaltliche Fehler bei der Datenverarbeitung an sich fallen jedoch nicht hierunter.

In diesen Fällen benötigen beide Seiten – Auftraggeber und Auftragnehmer – für die Verarbeitung eine „eigene“ Rechtsgrundlage nach Artikel 6 Absatz 1 beziehungsweise Artikel 9 Absatz 2 DS-GVO.

4. 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. So liegt beispielsweise keine Auftragsverarbeitung vor, wenn ein Copyshop den Auftrag erhält, einige T-Shirts mit Namen zu bedrucken. Hier bildet nicht die Verarbeitung der personenbezogenen Daten, sondern das farbliche Bedrucken der T-Shirts wie bei einem Druck mit Symbolen, Wappen,

Sinnsprüchen oder Ähnlichem den Schwerpunkt der Tätigkeit. In diesen Fällen liegt keine Auftragsverarbeitung im Sinne der DS-GVO vor. Die Datenverarbeitungen sind als „unvermeidliches Beiwerk“ bei der Erfüllung der eigentlichen Dienstleistungspflicht zu betrachten. Allerdings entfällt damit die unter Frage 3 dargestellte Privilegierung für die Datenverarbeitung des Auftragnehmers. In Folge dessen benötigt der Auftragnehmer in diesen Fällen für seine Datenverarbeitung eine „eigene“ Rechtsgrundlage nach Artikel 6 Absatz 1 beziehungsweise Artikel 9 Absatz 2 DS-GVO. Im Falle des Copyshops kann sich dieser auf Artikel 6 Absatz 1 Buchstabe f DS-GVO berufen, sofern nicht im Einzelfall die Interessen der Betroffenen überwiegen.

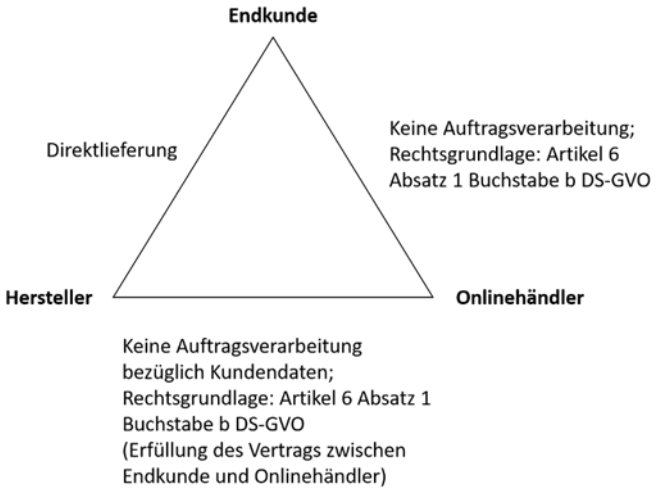
Beispiele:

- Ein Blumen- oder Weinhändler erhält **für die Versendung** von Blumen- beziehungsweise Weingeschenken an dritte Personen von seinem Kunden eine Liste mit Adressdaten der Empfänger. Als Rechtsgrundlage kommt für die Verarbeitung der personenbezogenen Daten Artikel 6 Absatz 1 Buchstabe f DS-GVO in Betracht. Von einem Überwiegen der Interessen der Betroffenen ist nicht auszugehen.

- Bei sogenannten „Dreiecksverhältnissen“, soweit es um die Beziehung zwischen Onlinehändler und Hersteller geht.

Beispiel:

Der Hersteller von Produkten erhält für mit Endkunden vereinbarte Direktlieferungen vom Online-Händler die Adresse des Kunden.



5. Für den Fall, dass die beabsichtigte Datenverarbeitung eine Auftragsverarbeitung nach Artikel 28 DS-GVO ist: In welcher Rolle befinde ich mich?

5.1 Auftraggeber

Ich bin Verantwortlicher (**Auftraggeber**), wenn ich die personenbezogenen Daten eigenverantwortlich verarbeite und dabei über die Zwecke („ob“, „wofür“, „warum“) und Mittel („wie“) entscheide. Dabei kann sich meine Rolle als Verantwortlicher auf Grund einer gesetzlichen oder vertraglichen Regelung sowie auch aus meiner faktischen Möglichkeit zur Einflussnahme auf die Entscheidungen ergeben. Eine Verantwortlichkeit scheidet hingegen aus, wenn ich in Bezug auf die konkrete Datenverarbeitung entweder *nur* den Zweck oder *nur* die (wesentlichen) Mittel festlege.

Die Bestimmung des Verantwortlichen und des von ihm festgelegten Zwecks ist für die Frage der Rechtmäßigkeit der Datenverarbeitung von zentraler Bedeutung. Artikel 5 Absatz 1 Buchstabe b DS-GVO verlangt, dass personenbezogen Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen. Auch ist eine Weiterverarbeitung dann unzulässig, wenn sie mit den ursprünglich festgelegten Zwecken nicht vereinbar ist.

Beispiele:

- Der Arbeitgeber ist berechtigt, die Personaldaten seiner Beschäftigten zu verarbeiten, die für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich sind.
- Das Unternehmen ist berechtigt, die Daten seiner Kunden zu verarbeiten, die für die Erfüllung des Vertrages mit dem Kunden erforderlich sind.

Ich bin ebenfalls Verantwortlicher (**Auftraggeber**), wenn ich mit weiteren Verantwortlichen als gemeinsam Verantwortliche nach Artikel 26 DS-GVO über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten entscheide. Ich verfüge dabei genauso wie die weiteren Verantwortlichen über die wesentliche Entscheidungsbefugnis hinsichtlich der konkreten Datenverarbeitung. Daneben besteht eine gewollte und bewusste Zusammenarbeit zwischen den weiteren Verantwortlichen und mir bezüglich der konkreten Datenverarbeitung. Dabei genügt es, wenn die weiteren Verantwortlichen und ich einen maßgeblichen und entscheidungserheblichen Beitrag zur Datenverarbeitung leisten. Außerdem muss die Verantwortlichkeit bei den anderen Beteiligten und mir nicht gleichwertig sein – eine Einbeziehung in verschiedenen Phasen der Verarbeitung und in unterschiedlichem Ausmaß ist möglich, sofern die Beiträge entscheidungserheblich bleiben. Es ist nicht erforderlich, dass bei einer gemeinsamen Verantwortlichkeit jeder Zugang zu den betreffenden personenbezogenen Daten hat.

5.2 Auftragnehmer

Ich bin Auftragsverarbeiter (**Auftragnehmer, Dienstleister**, **Leistungserbringer**), wenn ich eine Aufgabe (konkrete Dienstleistung zur Verarbeitung von personenbezogenen Daten) übertragen bekomme, bei der ausschließlich mein Auftraggeber über die Zwecke der Datenverarbeitung entscheidet. Über die Mittel der Datenverarbeitung entscheidet ebenfalls mein Auftraggeber, sofern mir nicht nach den Umständen des Einzelfalls ein Handlungsspielraum eingeräumt ist, über die Mittel der Datenverarbeitung („wie“) beziehungsweise über technische und organisatorische Fragen (mit) zu entscheiden. Dieses kann zum Beispiel die Entscheidung über die eingesetzte Soft- und Hardware zur Durchführung meines Auftrags sein. Inhaltliche Fragen, die den Kern der Rechtmäßigkeit der Verarbeitung der Daten betreffen sind allerdings meinem Auftraggeber vorbehalten (zum Beispiel welche Daten werden verarbeitet? Wie lange werden die Daten verarbeitet? Wer hat Zugang zu den Daten?).

Beispiele:

- Ein Lohnbuchhaltungsbüro führt für Kunden oder Mandanten die (reine) Lohn- und Gehaltsabrechnung durch;
- Ein Callcenter übernimmt bei der Kundenbetreuung eines Unternehmens nur Aufgaben ohne eigenen Handlungsspielraum, wie
    - Weitervermittlung der Kunden an die jeweils zuständige Stelle innerhalb des Unternehmens,
    - Aufnahme von Kontaktdaten oder sonstigen Informationen zwecks Weitergabe an die zuständige Stelle;
- Ein Dienstleister führt rein technische Dienstleistungen wie zum Beispiel Services zur Auswertung und Analyse von Webseiten oder zum Versenden von Newslettern, bei denen Nutzerdaten verarbeitet werden, durch;
- Ein Dienstleister führt Wartungsarbeiten an technischen Geräten mit der Möglichkeit des Zugangs zu personenbezogenen Daten durch (Anmerkung: Für weitere Hinweise siehe Antwort zu Frage 7 Buchstabe a).

Weitere Erläuterungen hierzu und Fallbeispiele finden Sie in den Leitlinien des EDSA zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ vom 07.07.2021.

6. Muss eine Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter geschlossen werden?

Ja. Für die Auftragsverarbeitung ist ein konkreter Rahmen festzulegen. Dafür müssen der Verantwortliche und der Auftragsverarbeiter in der Regel einen Vertrag zur Auftragsverarbeitung schließen. Alternativ kann sich der Auftragsverarbeiter zum Beispiel auch einseitig gegenüber dem Verantwortlichen verpflichten.

Diesbezüglich enthält Artikel 28 DS-GVO für die Ausgestaltung des Verhältnisses zwischen Verantwortlichem und Auftragsverarbeiter einzelne Vorgaben. Der Verantwortliche muss insbesondere einen Auftragsverarbeiter auswählen, der hinreichend Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet (Artikel 28 Absatz 1 DS-GVO).

Darüber hinaus ist in dem Vertrag beziehungsweise die sonstige Verpflichtung unter anderem nach Artikel 28 Absatz 3 Satz 1 DS-GVO Folgendes festzulegen:

- Gegenstand (zum Beispiel Erhebung von Kundendaten) und die Dauer der Verarbeitung (zeitlicher Rahmen von der Erhebung bis zur Löschung),
- Art und Zweck der Verarbeitung (zum Beispiel Vernichtung von Dokumenten),
- Art der personenbezogenen Daten,
- Kategorien betroffener Personen und
- Pflichten und Rechte des Verantwortlichen (insbesondere konkrete Festlegung der Weisungs- und Kontrollbefugnis).

Zudem müssen nach Artikel 28 Absatz 3 Satz 2 in Verbindung mit Artikel 32 DS-GVO Regelungen über die geeigneten technischen und organisatorischen Maßnahmen getroffen werden, mit denen ein angemessenes Schutzniveau erreicht werden kann. Diesbezüglich reicht ein einfacher Hinweis auf die allgemeinen Rechtsgrundlagen nicht aus. Stattdessen sind zumindest die durch den Auftragsverarbeiter anzuwendenden technischen und organisatorischen Maßnahmen, die Genehmigungspflicht des Verantwortlichen für diesbezügliche Änderungen sowie die Pflicht des Auftragsverarbeiters zur regelmäßigen Überprüfung der Maßnahmen im Hinblick auf deren weiterhin bestehende Angemessenheit aufzunehmen. Die Angaben müssen so detailliert sein, dass es dem Verantwortlichen möglich ist, die Angemessenheit der Maßnahmen im Hinblick auf das zu erreichende Schutzniveau bewerten zu können. Inwieweit der Verantwortliche diesbezüglich konkrete Vorgaben machen muss, hängt vom Einzelfall ab. So kann es ausreichen, dass der Verantwortliche lediglich das zu erreichenden Schutzniveau vorgibt. Für diesen Fall muss er jedoch die durch den Auftragsverarbeiter beabsichtigten technisch-organisatorischen Maßnahmen genehmigen.

Die Europäische Kommission hat Standardvertragsklauseln gemäß Art. 28 Abs. 7 DS-GVO für eine rein nationale Auftragsverarbeitung zwischen einem Verantwortlichen und einem Auftragsverarbeiter erarbeitet.

7. Unter welchen Voraussetzungen ist die Beauftragung eines Unter-Auftragnehmers zulässig?

Möchte der Auftragsverarbeiter seinerseits einen weiteren Dienstleister bei der Verarbeitung der personenbezogenen Daten in Anspruch nehmen, sind folgende Voraussetzungen zu erfüllen:

- Der Auftragsverarbeiter holt vor Einsatz des Unterauftragsverarbeiters die schriftliche Genehmigung des Verantwortlichen ein.
- Der Auftragsverarbeiter schließt mit dem Unterauftragsverarbeiter einen schriftlichen Vertrag, welcher dem Unterauftragsverarbeiter dieselben Pflichten auferlegt, wie sie der Verantwortliche dem Auftragsverarbeiter auferlegt.

Der Verantwortliche behält auch bei einer Unterauftragsverarbeitung die zentrale Rolle bei der Datenverarbeitung. Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen uneingeschränkt haftbar (Artikel 28 Abs. 4 DS-GVO).

Die vorherige schriftliche Genehmigung zur Einbeziehung eines Unterauftragsverarbeiters kann sich auf einen konkreten Unterauftragsverarbeiter zu einer bestimmten Verarbeitungstätigkeit beziehen. Alternativ kann bereits bei Vertragsschluss über die Auftragsverarbeitung eine Übereinkunft über die Zulässigkeit bestimmter Unterauftragsverarbeiter erfolgen, wobei eine Liste der zugelassenen Unterauftragsverarbeiter in den Vertrag aufgenommen werden sollte.

8. Antworten zu verschiedenen Einzelfällen:

8.1 Bedarf es für IT-Wartungsdienstleistungen eines Vertrags zur Auftragsverarbeitung?

Ja. Es liegt eine Auftragsverarbeitung vor. Nach der einheitlich abgestimmten Auffassung der Datenschutz-Aufsichtsbehörden des Bundes und der Länder ist dies der Fall, sofern nicht rein technische Wartungen der Infrastruktur vorgenommen werden. Denn im Rahmen der beauftragten Tätigkeit besteht für den Dienstleister zumindest die Möglichkeit des Zugriffs auf personenbezogene Daten der Beschäftigten des Auftraggebers oder auf Kundendaten, zum Beispiel bei Fehleranalysen, bei Remote-Zugriffen oder bei Support-Arbeiten. Auch liegt nicht die in der Antwort zu Frage 4 dargestellte Konstellation vor. Aufgrund der im Rahmen der Fernwartung bestehenden technischen Möglichkeit zur systematischen und umfassenden Verarbeitung personenbezogener Daten ist im

Hinblick auf die Leistung des Auftragnehmers stets ein entsprechender Schwerpunkt in der Datenverarbeitung zu sehen.

Das Kurzpapier Nummer 13 der Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder (DSK) gibt die einheitliche Position der deutschen Aufsichtsbehörden zur Auftragsverarbeitung nach Artikel 28 DS-GVO wieder und stellt unter dem Punkt „Wartung und Fernzugriffe“ die zu beachtenden Punkte zusammen.

8.2 Müssen innerhalb eines Konzerns Verträge zur Auftragsverarbeitung abgeschlossen werden, wenn ein Konzernunternehmen die Datenverarbeitung für andere Konzernunternehmen durchführt?

Es kommt darauf an:

Wenn die Datenverarbeitung bei konzerninternem Outsourcing zum Beispiel durch „Shared-Services-Gesellschaften“ (Tochter-, Schwester- oder Mutterunternehmen) erfolgt, ist die konkrete Ausgestaltung des Rechtsverhältnisses zwischen den Konzernunternehmen entscheidend.

- Sollte das datenverarbeitende Konzernunternehmen auf Grund der konkreten Auftragsregelung selbst Verantwortlicher sein (regelmäßig zum Beispiel bei weisungsfreien Personalentscheidungen für andere Konzernunternehmen), scheidet eine Auftragsverarbeitung aus. Als Rechtsgrundlage für die Datenverarbeitung durch das Konzernunternehmen kommt dann zumindest Artikel 6 Absatz 1 Buchstabe f DS-GVO in Betracht, wie Erwägungsgrund 48 zur DS-GVO verdeutlicht (Gegebenenfalls ist in diesen Fällen der Abschluss einer Vereinbarung im Rahmen einer gemeinsamen Verantwortlichkeit nach Artikel 26 DS-GVO notwendig).
- Sollte die Datenverarbeitung durch das Konzernunternehmen nicht als Verantwortlicher erfolgen, ist eine Auftragsverarbeitung möglich. Ein entsprechender Vertrag ist zu schließen, in welchem ausdrücklich die Weisungsgebundenheit und die Kontrollrechte für die konkreten Verarbeitungstätigkeiten geregelt sind.

Darüber hinaus gilt für das datenverarbeitenden Konzernunternehmen Folgendes:

Im Verhältnis zwischen dem datenverarbeitenden Konzernunternehmen und einer unternehmenseigenen Abteilung, bei der die Datenverarbeitung erfolgt, handelt regelmäßig nur das Konzernunternehmen als Verantwortlicher. In diesem Fall kann grundsätzlich keine Auftragsverarbeitung durch die Abteilung vorliegen. Der Auftragsverarbeiter muss immer eine andere (externe) Stelle als der Verantwortliche sein. Ein Vertrag zur Auftragsverarbeitung kommt daher nicht in Betracht.

8.3 Bedarf es eines Vertrages zur Auftragsverarbeitung, wenn eine Druckerei einen Auftrag von vorgefertigten Schriftstücken mit integrierten personenbezogenen Daten zum Druck erhält?

Nein. Die Dienstleistung der Druckerei ist keine Auftragsverarbeitung.

Die Beauftragung mit den beschriebenen fachlichen Dienstleistungen, also mit Dienstleistungen, bei denen die Datenverarbeitung nicht im Vordergrund steht, beziehungsweise bei denen die Datenverarbeitung nicht zumindest einen wichtigen (Kern-) Bestandteil ausmacht, stellt keine Auftragsverarbeitung im datenschutzrechtlichen Sinne dar. Als Rechtsgrundlage für die Datenverarbeitung durch die Druckerei kommt Artikel 6 Absatz 1 Buchstabe f DS-GVO in Frage.

Beispiele:

Ausdruck von bereits vorgefertigten Einladungsschreiben im PDF-Format inklusive Adressangaben.

Anders wäre der Fall zu beurteilen, wenn der Druckerei eine separate Datei mit Adressen zur Verfügung gestellt würde und die Einbindung dieser Adressen in das Druckwerk Bestandteil der Leistung der Druckerei wäre. Erst durch die Zusammenführung der personenbezogenen Daten (Adressdatensatz) mit dem Drucktext entsteht das zu versendende Endprodukt. In diesem Fall läge eine Auftragsverarbeitung vor.

8.4 Ist mit Steuerberatern ein Vertrag zur Auftragsverarbeitung zu schließen?

Nein. Steuerberater sind keine Auftragsverarbeiter im Sinne von Artikel 4 Nummer 8 DS-GVO. Dies ergibt sich aufgrund der besonderen berufsrechtlichen Vorgaben für Steuerberater. Danach haben Steuerberater ihre beruflichen Tätigkeiten weisungsfrei, eigenverantwortlich und unabhängig auszuüben [§ 11 Absatz 2 Satz 1 und Satz 2, § 32 Absatz 2 Satz 1 sowie § 57 des Steuerberatungsgesetzes (StBerG)]. Dies gilt auch, soweit sie zusätzlich Aufgaben im Rahmen der Lohn- und Gehaltsbuchhaltung wahrnehmen. Eine weisungsgebundene Tätigkeit im Sinne einer Auftragsverarbeitung nach Artikel 28 DS-GVO stünde den berufsrechtlichen Regelungen entgegen. Als Rechtsgrundlage für die Datenverarbeitung durch den Steuerberater kommt Artikel 6 Absatz 1 Buchstabe b DS-GVO in Verbindung mit § 11 Absatz 1 Satz 1 StBerG (gegebenenfalls für besondere Kategorien personenbezogener Daten in Verbindung mit Artikel 9 Absatz 2 Buchstabe g DS-GVO in Verbindung mit § 11 Absatz 2 Satz 3 StBerG) in Betracht.

8.5 Muss eine Kommune mit einer anderen öffentlichen Stelle, die sie mit der Gewährung von Beihilfen für ihre Beschäftigten beauftragt hat, einen Vertrag zur Auftragsverarbeitung schließen?

Es kommt darauf an:

Nein. Es liegt keine Auftragsverarbeitung vor, wenn diese Aufgabe von der Kommune auf eine der Aufsicht des Landes unterstehende juristische Person des öffentlichen Rechts als eigene Aufgabe übertragen worden ist (sogenannte „Zuständigkeitsübertragung“, siehe § 107 Absatz 6 Satz 2 des Niedersächsischen Kommunalverfassungsgesetzes – NKomVG).

Ja. Eine Auftragsverarbeitung ist gegeben, wenn es sich hierbei nur um eine Beauftragung zur Erbringung von Verarbeitungsleistungen und nicht um eine Übertragung als eigene Aufgabe handelt. Die Kommunen sind dabei an die in § 107 Absatz 6 NKomVG gesetzten Grenzen gebunden.

8.6 Muss mit Reinigungsunternehmen, die mit der Reinigung von Büroräumen beauftragt sind, ein Vertrag zur Auftragsverarbeitung geschlossen werden?

Nein. Es liegt keine Auftragsverarbeitung vor. Zur beauftragten Dienstleistung gehört nicht die Verarbeitung personenbezogener Daten. Vielmehr beschränkt sich die Aufgabe auf die Reinigungstätigkeit der vereinbarten Räume. Es wird empfohlen, dem Dienstleister aufzugeben, seine Beschäftigten für den Fall, dass diese bei der Reinigung von Büroräumen zufällig von personenbezogenen Daten Kenntnis erlangen, zur Verschwiegenheit zu verpflichten. Weitere Hintergründe zur Verpflichtung von Beschäftigten sind im Kurzpapier Nummer 19 der DSK enthalten.

9. Müssen Behörden oder sonstige öffentliche Stellen in Niedersachsen neben Artikel 28 DS-GVO Sonderregelungen zur Auftragsverarbeitung beachten?

Für Behörden und sonstige öffentliche Stellen, welche unter die JI-Richtlinie fallen,[2] gilt für die Auftragsverarbeitung zunächst die Regelung des § 45 Niedersächsisches Datenschutzgesetz (NDSG). Daneben sind besondere Rechtsvorschriften zu Auftragsverarbeitungen zu beachten, welche aufgrund

[2] „Richtlinie (EU) 2016/680 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates“

der Öffnungsklauseln in Artikel 6 Abs. 2 und Abs. 3 S. 1 Buchstabe b DS-GVO in Verbindung mit der jeweiligen spezialgesetzlichen Regelung gelten.

Beispiele:

- § 92 a des Niedersächsischen Beamtengesetzes enthält Sonderregelungen zur Verarbeitung von Personalaktendaten im Auftrag.
- § 80 des zehnten Buches Sozialgesetzbuch enthält Sonderregelungen zur Verarbeitung von Sozialdaten durch Sozialleistungsträger. Hiernach hat der Verantwortliche seiner Rechts- oder Fachaufsichtsbehörde den Inhalt, Umfang und Auftragnehmer der Auftragsverarbeitung rechtzeitig vor der Auftragserteilung anzuzeigen. Die Erteilung eines Auftrags zur Verarbeitung von Sozialdaten durch nicht-öffentliche Stellen ist mit Ausnahme von Verträgen über die Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen nur zulässig, wenn beim Verantwortlichen sonst Störungen im Betriebsablauf auftreten können oder die übertragenen Arbeiten beim Auftragsverarbeiter erheblich kostengünstiger besorgt werden können.

10. Kann ein Auftragsverarbeiter seinen Sitz auch außerhalb der Europäischen Union/des Europäischen Wirtschaftraums haben?

Ja, ein Verantwortlicher kann auch einen Auftragsverarbeiter in einem Land außerhalb der Europäischen Union auswählen. In diesem Fall sind allerdings die besonderen Vorgaben für einen Drittstaatstransfer nach Kapitel V der DS-GVO zu beachten. Danach dürfen personenbezogene Daten nur dann in Drittstaaten transferiert werden, wenn Verantwortliche und Auftragsdatenverarbeiter die im Kapitel V festgelegten Voraussetzungen erfüllen und auch die übrigen Grundsätze der DS-GVO eingehalten werden, damit das durch die DS-GVO gewährleistete Schutzniveau nicht untergraben wird. Dies kann z.B. durch den Abschluss der Standarddatenschutzklauseln des EDSA für eine internationale Auftragsverarbeitung und gegebenenfalls zusätzliche Maßnahmen zur Sicherstellung eines dem in der EU im Wesentlichen gleichwertigen Schutzniveaus erreicht werden. Bei Nutzung der unveränderten Standarddatenschutzklauseln der EU-Kommission vom Juni 2021 ist kein zusätzlicher nationaler Auftragsverarbeitungsvertrag nach Art. 28 DS-GVO erforderlich.[3]

Weitere Informationen zur internationalen Auftragsverarbeitung finden Sie hier.

[3] Bei der Verwendung der alten Standardvertragsklauseln aus dem Jahr 2010 war zusätzlich der Abschluss eines Auftragsverarbeitungsvertrags nach Art. 28 DS-GVO erforderlich. Diese alten Standardvertragsklauseln dürfen für Neuverträge nicht mehr verwendet werden. Spätestens bis zum 27.12.2022 müssen entsprechende Auftragsverarbeitungsverträge auf die neuen Standarddatenschutzklauseln umgestellt werden.

11. Unter welchen Umständen haftet ein Auftragsverarbeiter für einen entstandenen Schaden?

Ein Auftragsverarbeiter kann für seinen Verantwortungsbereich haftbar für durch die Verarbeitung entstandene Schäden sein (Artikel 82 Abs. 2 DS-GVO). Eine Haftung entsteht einerseits, wenn der Auftragnehmer die Grenzen seines Auftrags verlässt und die personenbezogenen Daten zu eigenen Zwecken verarbeitet und damit selbst zu einem Verantwortlichen wird (Art. 28 Abs. 10 DS-GVO). Andererseits haftet der Auftragsverarbeiter nur dann, wenn er eine der speziellen Pflichten für Auftragsverarbeiter nach Artikel 28 DS-GVO nicht erfüllt hat oder er gegen eine rechtmäßige Anweisung des Verantwortlichen gehandelt hat.

12. Was soll ich machen, wenn ich als Verantwortlicher unsicher bin und noch keinen Auftragsverarbeitungsvertrag abgeschlossen habe?

Sofern Sie eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten benannt haben, wenden Sie sich zunächst an diese oder diesen. Die oder der Datenschutzbeauftragte Ihres Hauses ist verpflichtet, Ihnen beratend zur Seite zu stehen.

Sofern eine Auftragsverarbeitung vorliegt, ist ein Auftragsverarbeitungsvertrag unverzüglich abzuschließen.

Liegt keine Auftragsverarbeitung und keine Rechtsgrundlage nach Artikel 6 Absatz 1 beziehungsweise Artikel 9 Absatz 2 DS-GVO vor, ist eine Datenverarbeitung in der Regel unzulässig. Bei Verstößen gegen den Grundsatz der Rechtmäßigkeit (Artikel 5 Absatz 1 Buchstabe a DS-GVO) kann nach Artikel 83 Absatz 5 DS-GVO ein Bußgeld verhängt werden.

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599
E-Mail an poststelle@lfd.niedersachsen.de schreiben