Auftragsverarbeitung

Auftragsverarbeitung tritt auf, wenn die Verarbeitung oder Speicherung von personenbezogenen Daten, die zwar für die eigenen Betriebszwecke erhoben wurden, an externe weisungsgebundene Unternehmen ausgelagert wird.

Verzeichnis von Verarbeitungstätigkeiten

Auch Auftragsverarbeiter müssen ein Verzeichnis von Verarbeitungstätigkeiten zu allen Kategorien von Tätigkeiten, die das externe Unternehmen im Auftrag durchführt. Die verpflichtenden Inhalte sind folgende:

- ✓ Name und Kontaktdaten des Unternehmens
- ✓ Name und Kontaktdaten des Datenschutzbeauftragten
- ✓ Verarbeitungskategorien
- ✓ Informationen zu etwaigen Übermittlungen an ein Drittland
- ✓ Beschreibung der technischen und organisatorischen Maßnahmen

Haftung

Betriebsleitung und Auftragsverarbeiter haften bei Datenschutzverstößen gemeinsam.

Auftragsverarbeitungsvertrag

Die Verarbeitung der Auftragsdaten erfolgt durch einen schriftlich geschlossenen Vertrag, der folgende Mindestangaben beinhalten muss:

- ✓ Gegenstand und Dauer des Auftrages
- ✓ Umfang, Zweck und Art der Datenverarbeitung
- ✓ Kategorien der zu verarbeitenden Daten
- ✓ Kategorien der betreffenden Personen
- ✓ Ergreifung von technischen und organisatorischen Maßnahmen
- ✓ Umfang der Weisungsbefugnisse
- ✓ Rückgabe von etwaigen Datenträgern nach Beendigung des Auftrages

Beispiele für Auftragsverarbeitung

- ❖ Inanspruchnahme von Cloud-Lösungen zur Datenspeicherung auf externen Servern
- ❖ Externe Akten-, Datenträgervernichtung
- ❖ Externe Lohnbuchhaltung
- ❖ Externe Backup- oder Archivdienstleistungen
- ❖ Hosting und Betreuung dynamischer Webseiten (z. B. Webseiten mit Kontaktformularen)

Handwerkskammer Ostwestfalen-Lippe zu Bielefeld
Gefördert durch: Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

Beispiele für Auftragsverarbeitung

(2/2)

- ☑ Externe Datenverarbeitung
- ☑ Externe Lohn- und Gehaltsabrechnung
- ☑ Externer Buchhaltungsservice
- ☑ Inanspruchnahme von Cloud-Lösungen zur Datenspeicherung auf externen Servern
- ☑ Auftragsdruck und -versand von Serienbriefen
- ☑ Externe Akten- und Datenträgerentsorgung
- ☑ Externe Backup- und Archivdienstleistungen
- ☑ Hosting und Betreuung dynamischer Webseiten, z. B. Webseiten mit Kontaktformularen
- ☑ Einscannen von Dokumenten durch Dienstleister
- ☑ Wartung und Fernzugriffe bei IT-Systemen oder TK-Anlagen mit Datenzugriff
- ☑ Beauftragung eines Callcenters zur Kundenkommunikation

Beauftragung von

- ☒ Berufsgeheimnisträger, wie Steuerberater, Wirtschaftsprüfer, Rechtsanwälte, Betriebsärzte, etc.
- ☒ Externe Datenschutzbeauftragte
- ☒ Personalvermittlung nach Auftrag
- ☒ Reinigung von Berufskleidung mit Namensschildern
- ☒ Geldtransfer durch Banken oder Sparkassen
- ☒ Transport- oder Kurierdienste
- ☒ Handwerkseinsätze in Unternehmen oder im Fremdauftrag
- ☒ Sachverständigentätigkeit, Erstellung Schadensgutachten

Handwerkskammer Ostwestfalen-Lippe zu Bielefeld

Gefördert durch: Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

Auftragsverarbeitungsvertrag

- ein Formulierungsvorschlag des ZDH

1. **Gegenstand und Dauer des Auftrages**
   entsprechend individueller Vereinbarung

2. **Umfang, Zweck und Art der Datenverarbeitung**
   „Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im sachlichen und zeitlichen Rahmen dieses Auftrages sowie nach Weisung des Auftraggebers. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

   Die Verarbeitung der Daten auch durch Unterauftragnehmer findet

   ☐ ausschließlich im Gebiet der Bundesrepublik Deutschland,

   ☐ in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum,

   ☐ In einem Drittstaat, und zwar _____ statt.

   In letzterem Fall weist der Auftragnehmer für die Rechtmäßigkeit entsprechenden vertragliche oder sonstige, der DSGVO entsprechenden Rechtsgrundlagen nach.“

3. **Technische und organisatorische Maßnahmen**

   „Der Auftragnehmer wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftragnehmers treffen, die den gesetzlichen Anforderungen genügen. Hierbei sind die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Die technisch-organisatorischen Maßnahmen des Auftragnehmers sind gesondert in diesem Vertrag festzulegen und Bestandteil des Vertrages.

   Der Auftragnehmer gewährleistet ein Verfahren zur Überprüfung der technischen und organisatorischen Maßnahmen. Er ist verpflichtet, die technischen und organisatorischen Maßnahmen an den Stand der Technik anzupassen, soweit dies erforderlich und wirtschaftlich zumutbar ist. Der Auftraggeber ist über wesentliche Änderungen vorab zu informieren. Die Änderungen sind schriftlich niederzulegen und werden Vertragsbestandteil. Vorschläge von Auftraggeber-Seite für Änderungen hat der Auftragnehmer zu prüfen. Der Auftraggeber ist über das Ergebnis zu informieren.

Handwerkskammer Ostwestfalen-Lippe zu Bielefeld
Gefördert durch: Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

Beauftragt der Auftragnehmer zur Erfüllung seiner vertraglichen Pflichten einen Unterauftragnehmer, stellt er sicher, dass die erforderlichen technischen und organisatorischen Maßnahmen von dem Unterauftragnehmer getroffen werden und dem Stand der Technik entsprechen."

4. Berichtigung, Sperrung und Löschung von Daten, Auskunft über Daten

„Der Auftragnehmer hat die Daten nach Weisung des Auftraggebers zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Sperrung oder Löschung seiner Daten wendet, leitet der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiter. Selbiges gilt für Auskunftsersuche."

5. Kontrollen und sonstige Pflichten des Auftragnehmers

„Der Auftragnehmer ist verpflichtet, das Datengeheimnis sowie etwaige berufliche Verschwiegenheitsverpflichtungen zu wahren. Er hat bei der Verarbeitung ausschließlich Beschäftigte einzusetzen, die entsprechend verpflichtet und geschult sind. Er hat insbesondere sicherzustellen, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung dieses Vertrages betraut sind, sorgfältig ausgewählt werden, die gesetzlichen Datenschutzbestimmungen beachten und die von dem Auftraggeber erlangten Informationen nicht unbefugt an Dritte weitergeben oder anderweitig verwerten.

Der Auftragnehmer nennt dem Auftraggeber die Ansprechperson für sämtliche vertragsrelevanten Angelegenheiten des Datenschutzes. Der Auftragnehmer hat Frau/ Herrn _____ als betrieblichen Datenschutzbeauftragten bestellt.

Der Auftragnehmer ist verpflichtet, ein Verarbeitungsverzeichnis gemäß Art. 30 Abs. 2 DSGVO zu führen. Der Auftragnehmer gewährt der Landesdatenschutzbeauftragten Zugang zu den Arbeitsräumen und unterwirft sich der Kontrolle nach Maßgabe des Landesdatenschutzgesetzes in seiner jeweiligen Fassung. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontroll- und Ermittlungshandlungen der Aufsichtsbehörde."

6. Unterauftragsverhältnisse

„Der Auftraggeber genehmigt die gesondert aufgelisteten Unterauftragsverhältnisse, die der Auftragnehmer vor Abschluss dieser Vereinbarung begründet hat. Über Änderungen hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Abschluss neuer Unterauftragsverhältnisse bedarf der vorherigen Zustimmung des Auftraggebers.

Der Auftragnehmer hat dem Unterauftragnehmer dieselben Pflichten aufzuerlegen, die er selbst gegenüber dem Auftraggeber zu erfüllen hat. Der Unterauftragnehmer ist sorgfältig auszuwählen. Der Auftragnehmer haftet gegenüber dem Auftraggeber vollumfänglich für Datenverstöße seiner Unterauftragnehmer."

7. Kontrollrechte des Auftraggebers

„Der Auftraggeber hat das Recht, vor Beginn und während der Datenverarbeitung die Einhaltung der von dem Auftragnehmer sowie von den Unterauftragnehmern getroffenen technischen und organisatorischen Maßnahmen zu kontrollieren oder von zu benennenden Prüfern kontrollieren zu lassen. Das Ergebnis ist zu dokumentieren.

Der Auftragnehmer gewährleistet die Möglichkeit zur Kontrolle. Hierzu weist er dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGO nach. Der Nachweis kann durch Vorlage aktueller Testate oder durch Berichte unabhängiger Prüfer (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Datenschutzauditoren, Qualitätsauditoren) erbracht werden.

Haben sich der Auftragnehmer und die von ihm beauftragten Unterauftragnehmer Verhaltensregeln unterworfen oder ein Zertifizierungsverfahren erfolgreich durchlaufen, sind sie verpflichtet, dem Auftraggeber dies nachzuweisen. Zertifikate sind zu aktualisieren.

Der Auftraggeber ist berechtigt, Stichprobenkontrollen durchzuführen. Diese sind anzukündigen. Würde die Ankündigung den Zweck der Prüfung gefährden oder besteht ein dringender Anlass zur Kontrolle, ist eine Ankündigung entbehrlich.“

8. Mitteilung bei Verstößen

„Der Auftragnehmer meldet dem Auftraggeber unverzüglich sämtliche Verstöße gegen Pflichten aus diesem Vertrag. Dies gilt insbesondere bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung bzw. zum Ausschluss möglicher nachteiliger Folgen für die Betroffenen zu ergreifen.“

9. Weisungsbefugnis des Auftraggebers

„Der Auftraggeber ist berechtigt, dem Auftragnehmer jederzeit Weisungen zu erteilen, insbesondere hinsichtlich der Art, des Umfangs und des Zeitpunkts der Verarbeitung von Daten. Die Weisungen des Auftraggebers erfolgen in Textform.

Erachtet der Auftragnehmer eine Weisung des Auftraggebers als rechtswidrig, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Er ist berechtigt, die Durchführung der Weisung auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Erteilt der Auftraggeber Einzelanweisungen bzgl. des Umgangs mit personenbezogenen Daten, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, z. B. Änderungen der technischen und organisatorischen Maßnahmen, werden sie als Auftrag auf Leistungsänderung behandelt.“

10. Löschung von Daten und Rückgabe von Datenträgern

„Der Auftragnehmer hat dem Auftraggeber sämtliche in seinem Besitz befindlichen personenbezogenen Daten, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, unverzüglich nach Erfüllung des Vertrages oder nach Aufforderung durch den Auftraggeber, spätestens mit Beendigung der Zusammenarbeit auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Ein Zurückbehaltungsrecht ist ausgeschlossen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind von dem Auftragnehmer entsprechend der geltenden Aufbewahrungsfristen hinaus aufzubewahren."

Dieses Muster dient der Orientierung und als Formulierungshilfe. Abweichungen ergeben sich aus der individuellen Auftragsgestaltung zwischen Auftraggeber und -nehmer.

Quelle: ZDH