DATENSCHUTZ – D12

Stand: August 2023

Ihr Ansprechpartner
Ass. iur. Kim Pleines
E-Mail
kim.pleines@saarland.ihk.de
Tel.
(0681) 9520-640
Fax
(0681) 9520-690

Auftragsverarbeitung nach der DSGVO

Immer mehr Unternehmen lagern ihre Datenverarbeitung, um Kosten und Zeit zu sparen, aus. Hierbei werden in der Regel personenbezogene Daten von externen Dritten weiterverarbeitet. Eine solche Verarbeitung unterliegt strengen Voraussetzungen. Zentrale Vorschrift ist Art. 28 DSGVO.

Auftragsverarbeitung - Was ist das?

Eine Auftragsverarbeitung (AV) liegt vor, wenn personenbezogene Daten im Auftrag für einen Verantwortlichen verarbeitet werden. Das ist typischerweise der Fall, wenn ein Externer beauftragt wird, die Kommunikation mit Kunden durchzuführen, etwa durch ein Call-Center, bei der (Fern-)Wartung von IT-Systemen oder im Bereich Personalverwaltung. Da die Möglichkeit besteht, dass der Dienstleister Zugriff auf personenbezogenen Daten erhält, ist mit dem Dienstleister ein Vertrag abzuschließen, der die Rechte und Pflichten regelt.

Welche Anforderungen bestehen an den Vertrag? Was muss geregelt sein?

Ein AV-Vertrag ist nicht zwingend vorgeschrieben. Ausreichend ist auch ein anderer Rechtsakt wie beispielsweise eine einseitig bindende Verpflichtung. Der AV-Vertrag (oder der Rechtsakt) muss **schriftlich** abgeschlossen werden; die elektronische Form reicht ebenfalls aus. In ihm muss der **Gegenstand** und die **Dauer** der Verarbeitung, **Art und Zweck der Verarbeitung,** die **Art** der personenbezogenen **Daten**, die **Kategorien** betroffener **Personen** und die **Pflichten und Rechte des Verantwortlichen** festgelegt werden.

Der Auftragsverarbeiter muss sorgfältig und unter Berücksichtigung der technischen und organisatorischen Maßnahmen ausgewählt werden.

Folgende Punkte müssen im Vertag **geregelt** sein:

Industrie- und Handelskammer des Saarlandes
Postanschrift: IHK Saarland │ 66104 Saarbrücken │ Büroanschrift: Franz-Josef-Röder-Straße 9 │ 66119 Saarbrücken
Tel. 0681/9520-0 │ Fax 0681/9520-888 │ E-Mail: info@saarland.ihk.de │ Internet: www.saarland.ihk.de

1. Personenbezogene Daten dürfen nur auf Weisung des Verantwortlichen verarbeitet werden. Die Weisungen sind zu dokumentieren.

2. Für die Datenverarbeitung sind ausschließlich Personen einzusetzen, die sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3. Der Auftragsverarbeiter muss alle technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO ergreifen.

4. Die Einschaltung von **Subunternehmen** bedarf der Genehmigung des Verantwortlichen. Mit dem Subunternehmen ist ebenfalls ein Vertrag abzuschließen. Der Auftragsverarbeiter steht für Datenschutzverstöße des Subunternehmers vollumfänglich ein.

5. Der Auftragsverarbeiter ist zu verpflichten, den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen, wenn Betroffene ihre Rechte geltend machen.

6. Der Auftragsverarbeiter ist zu verpflichten, den Verantwortlichen dabei zu unterstützen, seine technischen und organisatorischen Maßnahmen zu erfüllen, Datenpannen zu melden und eine Datenschutz-Folgenabschätzung durchzuführen.

7. Nach Abschluss der Verarbeitung sind alle personenbezogenen Daten entweder zu löschen oder zurückzugeben.

8. Der Verarbeiter muss dem Verantwortlichen Überprüfungen/Kontrollen ermöglichen.

Welche Pflichten hat der Auftraggeber/Verantwortliche?

Der Auftraggeber bleibt verantwortlich für die Datenverarbeitung. Durch die Beauftragung eines Dritten kann er sich nicht von der Verantwortlichkeit befreien. Der Auftraggeber muss seinen Auftragnehmer sorgfältig auswählen. Er darf sich nur solcher Auftragsverarbeiter bedienen, die hinreichende Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz verwenden.

Der Auftraggeber ist zudem dazu verpflichtet, den Betroffenen darüber informieren, wer Empfänger der personenbezogenen Daten ist. Macht der Betroffene von seinem Auskunftsrecht oder einem anderen Recht Gebrauch, ist er zur Erfüllung verpflichtet.

➔**D05** „Informationspflichten nach der DSGVO“, Kennzahl 2356
➔**D13** „Auskunftsersuchen nach der DSGVO“, Kennzahl 2356

Welche Pflichten hat der Auftragsverarbeiter?

Der Auftragsverarbeiter muss selbst die Grundsätze der DSGVO einhalten. Er muss – genau wie der Verantwortliche – **Verfahrensverzeichnisse** führen, mit der Aufsichtsbehörde zusammenarbeiten und **technische und organisatorische Maßnahmen** ergreifen. Er handelt bei der Datenverarbeitung ausschließlich **auf Weisung** des Verantwortlichen/Auftraggeber. Verletzungen des Schutzes personenbezogener Daten sind nach Bekanntwerden unverzüglich dem Auftraggeber zu melden.

Wer haftet bei Datenschutzverstößen?

Grundsätzlich haften der **für die Verarbeitung Verantwortliche und der Auftragsverarbeiter** gemeinsam für materielle oder immaterielle Schäden, die aufgrund eines Verstoßes gegen die DSGVO entstanden sind. Die Haftung des Auftragsverarbeiters beschränkt sich auf Verstöße gegen speziell dem Auftragsverarbeiter auferlegte Pflichten. Er kann sich jedoch von einer Haftung freistellen, wenn er nachweisen kann, dass er für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich ist.

Neben der Haftung auf Schadensersatz können sowohl gegen den Auftraggeber als auch den Auftragsverarbeiter Geldbußen von bis zu 10 Millionen Euro oder 2 % des gesamten weltweit erzielten Jahresumsatzes verhängt werden. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag werden in jedem Einzelfall unter anderem die Art, Schwere und Dauer des Verstoßes berücksichtigt, ob der Verstoß fahrlässig oder vorsätzlich erfolgte und den Grad der Verantwortung.

Beispiele für eine Auftragsverarbeitung

- Erstellung von Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Externe
- Software as a Service/Cloud-Services, sofern personenbezogene Daten verarbeitet werden
- Verarbeitung von Kundendaten durch ein Callcenter
- Daten(träger)entsorgung durch Dienstleister
- (Fern-)Wartung von Datenverarbeitungsanlagen

Beispiele, wann kein Auftragsverarbeitung vorliegt

- Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte etc.)
- Inkassobüros mit Forderungsübertragung,
- Bankinstituts für den Geldtransfer,
- Postdienstes für den Brieftransport