DATENSCHUTZ – D12

Stand: März 2018

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 personenbezogene Daten von externen Dritten weiterverarbeitet. Eine solche Auftragsverarbeitung unterliegt strengen Voraussetzungen. Zentrale Vorschrift ist Art. 28 DSGVO, der den bisherigen § 11 BDSG ablöst. Nicht nur der Name hat sich geändert, aus „Auftragsdatenverarbeitung“ wird „Auftragsverarbeitung“, auch inhaltlich ergeben sich einige Unterschiede bzw. Neuerungen im Vergleich zur alten Regelung. Neu ist, dass der **Auftragsverarbeiter** stärker in die Pflicht genommen wird. Es ist insbesondere dazu verpflichtet, ein **eigenes Verfahrensverzeichnis** anzulegen.

➔**D11** „Verzeichnis von Verarbeitungstätigkeiten“, **Kennzahl 2158**

Die im BDSG-alt häufig verwendete Figur der sog. **Funktionsübertragung** in Abgrenzung zur Auftrags(daten)verarbeitung ist in der DSGVO nicht vorgesehen. Eine Funktionsübertragung liegt nach bisherigem Recht vor, wenn der Verarbeiter Aufgaben/Funktionen wahrgenommen hat, die über eine bloße Datenverarbeitung als solche hinausgehen und er eine gewisse Entscheidungsfreiheit dabei hat. Nach dem Wortlaut der DSGVO schließt ein gewisser Entscheidungsspielraum eine Auftragsverarbeitung nicht aus. Ob an der Figur festgehalten werden kann, wird die Zukunft zeigen.

Auftragsverarbeitung - Was ist das?

Eine Auftragsverarbeitung (ADV) liegt vor, wenn personenbezogene Daten im Auftrag für einen Verantwortlichen verarbeitet werden. Auftragsverarbeitungen kommen insbesondere bei der Wartung von IT-Systemen oder im Bereich Personalverwaltung zum Einsatz.

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

Die Auftragsverarbeitung nach der DSGVO ist **beschränkt „privilegiert“**. Die Verarbeitung stellt keine Übermittlung an einen Dritten dar. Auch nach der DSGVO bedarf die Übermittlung der Rechtfertigung. Eine Vorschrift, die die Beteiligten von dem grundsätzlich geltenden Verbotsprinzip befreit, Daten nicht ohne Einwilligung oder aufgrund eines Erlaubnistatbestandes zu verarbeiten, gibt es - anders als im BDSG - in der DSGVO nicht. Eine Übermittlung wird jedoch regelmäßig aufgrund „berechtigter Interessen“ nach Art. 6 Abs. 1 lit. f DSGVO zulässig sein. Alternativ kann auch Art. 28 DSGVO als eigenständige Befugnisnorm für die Verarbeitung der Daten angesehen werden. Sieht man die Verarbeitung als einheitlichen Vorgang der Datenverarbeitung, richtet sich die Rechtfertigung ebenfalls nach den berechtigten Interessen.

Ein Auftragsverarbeitungsvertrag ist **typischerweise abzuschließen**, wenn ein Externer beauftragt wird, die Kommunikation mit Kunden durchzuführen, etwa durch Call-Center oder wenn die Lohn- und Gehaltsabrechnung outgesourct wird. Aber auch bei der IT-Wartung oder Fernwartung von Systemen, bei der die Möglichkeit besteht, Zugriff auf personenbezogenen Daten zu erhalten, muss ein ADV-Vertrag abgeschlossen werden. Nicht darunter fallen rein technische Wartungen wie z. B. Arbeiten an der Klimaanlage.

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

Ein ADV-Vertrag ist nicht zwingend vorgeschrieben. Ausreichend ist auch ein anderer Rechtsakt wie beispielsweise eine einseitig bindende Verpflichtung. Der ADV-Vertrag (oder der Rechtsakt) muss jedoch **schriftlich** abgeschlossen werden. Die elektronische Form reicht 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 - wie bisher auch - sorgfältig und unter Berücksichtigung der technischen und organisatorischen Maßnahmen ausgewählt werden.

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

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.

Wichtig: *Bereits abgeschlossene Verträge sind zu überprüfen und gegebenenfalls den Anforderungen in Art. 28 DSGVO anzupassen. Beim Abschluss von Neuverträgen sollte die zum 25.05.2018 eintretende Rechtslage jetzt schon beachtet werden.*

Welche Pflichten hat der Auftraggeber/Verantwortliche?

Der Auftraggeber muss, wie bislang auch, 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 hat bei der Auftragsverarbeitung zwar **Kontrollrechte,** aber keine Kontroll- oder Dokumentationspflichten mehr wie nach dem BDSG. Die entsprechenden Vorschriften aus dem BDSG wurden durch die DSGVO nicht übernommen.

Daten, die aufgrund gesetzlicher oder berufsrechtlicher Geheimhaltungspflichten vertraulich zu behandeln sind, dürfen nicht offenbart werden.

Der Auftraggeber ist zu gesonderten **Informations- und Mitteilungspflichten** verpflichtet. Er muss insbesondere den Betroffenen darüber informieren, wer Empfänger der personenbezogenen Daten ist.

➔**D05** „Informationspflichten nach der DSGVO“, **Kennzahl 2158**

Welche Pflichten hat der Auftragsverarbeiter?

Der Auftragsverarbeiter unterliegt künftig mehr Pflichten und muss selbst die Grundsätze der DSGVO einhalten. War der Auftraggeber nach dem BDSG ausschließlich für die Datenverarbeitung verantwortlich, so ist nunmehr auch der Auftragsverarbeiter mit in die Verantwortung für die Verarbeitung der Daten genommen worden Er muss - genau wie der Verantwortliche - **Verfahrensverzeichnisse** führen und mit der Aufsichtsbehörde zusammenarbeiten. Er hat die Pflicht, **technische und organisatorische Maßnahmen** zu ergreifen und (in der Regel) einen **betrieblichen Datenschutzbeauftragten** zu bestellen.

Wie bislang auch ist der Auftragsverarbeiter grundsätzlich verpflichtet bei der Datenverarbeitung ausschließlich **auf Weisung** des Verantwortlichen zu handeln. Aus diesem Grund ist er nicht Dritter im Sinne der Art. 4 Nr. 10 DSGVO, sondern Empfänger, Art. 4 Nr. 9 DSGVO. Verletzungen des Schutzes personenbezogener Daten sind nach Bekanntwerden unverzüglich dem Verantwortlichen zu melden.

Hat der Auftragsverarbeiter keine Niederlassung in der EU, muss er einen Vertreter in der EU bestellen.

Wer haftet bei Datenschutzverstößen?

Nach Art. 82 DSGVO haftet der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter für materielle oder moralische Schäden auf Schadensersatz, die aufgrund eines Verstoßes gegen die DSGVO entstanden sind. Grundsätzlich haften der **für die Verarbeitung Verantwortliche und der Auftragsverarbeiter** gemeinsam. 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.

Verstößt der Auftragsverarbeiter gegen Weisungen, in dem er die Daten des Auftraggebers für eigene Zwecke oder Zwecke Dritter verarbeitet, gilt er selbst als Verantwortlicher mit allen rechtlichen Folgen. Neben der Pflicht zur Erfüllung der Informationspflichten und der Betroffenenrechte, drohen ihm Geldbußen von bis zu 10 Millionen Euro oder 2 % des gesamten weltweit erzielten Jahresumsatzes. 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.