https://www.activemind.de/magazin/pflichten-auftragsverarbeiter-dsgvo/

Die Verarbeitung von Daten im Auftrag bringt für den Auftragsverarbeiter einige Pflichten mit sich. Während nach dem Bundesdatenschutzgesetz (BDSG) ausschließlich der Auftraggeber für die Auftragsverarbeitung (vormals: Auftragsdatenverarbeitung) verantwortlich war, wird der Auftragsverarbeiter mit Wirksamkeit der Datenschutz-Grundverordnung (DSGVO) für die Verarbeitung personenbezogener Daten mitverantwortlich. Auf einige Punkte sollten Dienstleister bei der Auftragsverarbeitung besonders achten – sonst drohen neben der Inanspruchnahme auf Schadensersatz ebenfalls empfindliche Strafen!

Vertragliche Pflichten des Auftragsverarbeiters

Wichtig ist zunächst der Abschluss eines Vertrages zur Auftragsverarbeitung nach Art. 28 DSGVO. Ohne einen solchen schriftlichen Vertrag besteht überhaupt keine Rechtsgrundlage für die Auftragsverarbeitung (AV).

Neben gewissen Mindestangaben rund um die datenschutzrechtlichen Rahmenbedingungen des Auftrages, muss dieser Auftragsverarbeitungs-Vertrag die in Art. 28 Abs. 3 S. 2 DSGVO festgelegten Mindestanforderungen der Pflichten des Auftragsverarbeiters beinhalten. Ohne diese Mindestangaben ist die gesamte Auftragsverarbeitung mangels Rechtsgrundlage unwirksam:

Weisungsgebundene Datenverarbeitung

Der Vertrag muss eine Regelung vorsehen, welche den Auftragsverarbeiter verpflichtet, nur nach Weisung des Verantwortlichen personenbezogene Daten zu verarbeiten. Dabei muss in verständlicher Weise hervorgehen, wie der Auftragnehmer vorgehen darf. Sollte der Auftragsverarbeiter einer Rechtsordnung unterliegen, welche ihn zur Datenverarbeitung verpflichtet, obwohl keine entsprechende Weisung vorgesehen ist, hat er den Verantwortlichen über diese Verarbeitungspflicht zu informieren.

Wahrung des Datengeheimnisses

Der Auftragnehmer hat zu gewährleisten, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden.

Technisch organisatorische Maßnahmen

Vertraglich festzulegen ist weiterhin die Pflicht, alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit zu ergreifen. Dabei sind die genauen vorzunehmenden Maßnahmen so konkret wie möglich zu beschreiben, da sie insbesondere darüber Auskunft geben sollen, ob möglicherweise ein Pflichtverstoß vorliegt.

Neben der tatsächlichen Umsetzung technischer und organisatorischer Maßnahmen muss der Auftragsverarbeiter nach Art. 28 Abs. 1 DSGVO gegenüber dem Verantwortlichen entsprechende Garantien bieten. Mithilfe dieser Garantien soll der Auftragsverarbeiter nachweisen können, dass durch diese technischen und organisatorischen Maßnahmen eine rechtmäßige Datenverarbeitung nach DSGVO erfolgt und die Rechte der Betroffenen ausreichend berücksichtigt werden.

Hinreichende Garantien können nach Art. 28 Abs. 5 DSGVO im Wege der Einhaltung genehmigter Verhaltensregelung gem. Art. 40 DSGVO oder mittels eines genehmigten Zertifizierungsverfahrens gem. Art. 42 DSGVO, beispielsweise eine ISO 27001-Zertifizierung, nachgewiesen werden. Hierbei handelt es sich jedoch nur um widerlegbare Garantien. Sie stellen also lediglich ein Indiz dafür da, dass eine rechtmäßige Datenverarbeitung erfolgt und die Betroffenenrechte gewahrt werden.

Inanspruchnahme von weiteren Auftragsverarbeitern (Subunternehmern)

Nach BDSG war bisher im Vertrag nur festzulegen, ob der Auftragnehmer überhaupt einen weiteren Auftragsverarbeiter beauftragen durfte. Nach Art. 28 Abs. Abs. 2 DSGVO ist nun vertraglich zu regeln, dass weitere Auftragsverarbeiter nur dann beauftragt werden dürfen, wenn entweder eine vorherige gesonderte oder eine allgemeine schriftliche Genehmigung des Verantwortlichen erteilt wird. Im Falle einer allgemeinen schriftlichen Genehmigung ist der Auftragsverarbeiter zu verpflichten, den Verantwortlichen vor jeder Beauftragung oder Änderung eines bereits bestehenden Auftrags hierüber zu informieren.

Zwischen dem Auftragsverarbeiter und den weiteren Auftragsverarbeitern muss ebenfalls ein Auftragsverarbeitungs-Vertrag abgeschlossen werden, welcher den Anforderungen des Art. 28 DSGVO genügt und die Datenschutzpflichten des Vertrages zwischen dem Verantwortlichen und dem primären Auftragsverarbeiter nicht unterschreitet.

Anträge betroffener Personen

Betroffene Personen haben gegenüber dem Verantwortlichen Ansprüche auf Auskunft, Berichtigung und Löschung von Daten, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch. Damit der Betroffene seine Rechte umfassend geltend machen kann, ist der Auftragsverarbeiter zu verpflichten, den Verantwortlichen bei der Wahrnehmung der Beantwortung dieser Ansprüche zu unterstützen. Hierzu hat der Auftragsverarbeiter die Gesuche der betroffenen Personen an den Verantwortlichen weiterzuleiten und in Umsetzung des Anspruchs entsprechende Weisungen, beispielsweise die Berichtigung von Daten, umzusetzen.

Unterstützung des Verantwortlichen

Der Auftragsverarbeiter muss gemäß Art. 28 Abs. 3 lit. f) DSGVO vertraglich verpflichtet werden, den Verantwortlichen dabei zu unterstützen, dessen Pflichten aus Art. 32 bis 36 DSGVO einzuhalten. Diese Pflichten beinhalten die Ergreifung der technischen und organisatorischen Maßnahmen (Art. 32 DSGVO), Meldung von Datenschutzverletzungen an Aufsichtsbehörden (Art. 33 DSGVO), Benachrichtigung der von Datenschutzverletzungen betroffenen Personen (Art. 34 DSGVO), Unterstützung bei einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) sowie Konsultierung der Aufsichtsbehörde bei Verarbeitungen mit hohen Risiken (Art. 36 DSGVO).

Lösch- und Rückgabepflichten nach Auftragsbeendigung

Der Auftragsverarbeitungs-Vertrag muss eine Bestimmung darüber enthalten, ob nach Beendigung des Auftrages der Auftragsverarbeiter alle personenbezogenen Daten zu löschen oder zurückzugeben hat, sofern nicht eine gesetzliche Verpflichtung zur Speicherung dieser Daten besteht.

Informationspflichten und Ermöglichung von Überprüfungen

Nachdem die DSGVO dem Verantwortlichen eine Auswahlpflicht auferlegt, wonach der Verantwortliche nur geeignete Auftragsverarbeiter beauftragen darf, muss sich der Verantwortliche über die Geeignetheit im Wege von Überprüfungen vergewissern können.

Da das Gesetz keine entsprechenden Duldungs- und Mitwirkungspflichten von Seiten des Auftragsverarbeiters vorsieht, muss der Vertrag solche Duldungs- und Mitwirkungspflichten schaffen. Damit der Auftragsverarbeiter nachweisen kann, dass er seine Pflichten aus Art. 28 DSGVO einhält, muss er dem Verantwortlichen alle hierfür erforderlichen Informationen zur Verfügung stellen und Überprüfungen durch den Verantwortlichen oder einen anderen von ihm beauftragten Prüfer (z. B. den externen Datenschutzbeauftragten des Verantwortlichen) ermöglichen.

Gesetzliche Pflichten des Auftragsverarbeiters

Neben den Pflichten des Auftragsverarbeiters, welche zwingend im Auftragsverarbeitungs-Vertrag geregelt sein müssen, bestehen weitere gesetzliche Pflichten:

Verzeichnis von Verarbeitungstätigkeiten

Jeder Auftragsverarbeiter muss ein schriftliches oder elektronisches Verzeichnis über alle Verarbeitungstätigkeiten der Auftragsverarbeitung führen. Hierzu sieht Art. 30 Abs. 2 DSGVO den erforderlichen Inhalt vor. Dieses Verzeichnis ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Zusammenarbeit mit der Aufsichtsbehörde

Art. 31 DSGVO verpflichtet den Auftragsverarbeiter auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen zu arbeiten. Diese Pflicht gilt jedoch nur hinsichtlich Sachverhaltsaufklärungen, die sich ausschließlich mithilfe des Auftragsverarbeiters erreichen lassen. Eine bloße Arbeitserleichterung der Aufsichtsbehörde ist hiermit nicht gemeint.

Bestellen eines Datenschutzbeauftragten

Der Auftragsverarbeiter hat unter den Voraussetzungen des Art. 37 Abs. 1 DSGVO einen (internen oder externen) Datenschutzbeauftragten zu benennen (mehr dazu im kostenlosen Whitepaper zum betrieblichen Datenschutzbeauftragten nach DSGVO).

Vertreter für Auftragsverarbeiter in Drittländern

Auftragsverarbeiter, die keine Niederlassung in der EU haben und personenbezogene Daten von EU-Bürgern verarbeiten, müssen gem. Art. 27 Abs. 1 DSGVO schriftlich einen Vertreter in der Union bestellen.

Übermittlungen von Daten an Drittländer und internationale Organisationen

Der Auftragsverarbeiter hat ebenfalls die Beschränkungen für Datenübermittlungen an Drittländer und internationale Organisationen gem. Art. 44 DSGVO zu beachten. Hiernach

dürfen personenbezogene Daten nur dann übermittelt werden, wenn die Verarbeitung insgesamt den Anforderungen der DSGVO genügt und im Empfängerland vergleichbare datenschutzrelevante Schutzmechanismen für Betroffene vorgesehen sind.

Risiken des Auftragsverarbeiters

Haftung des Auftragsverarbeiters

Der Dienstleister haftet als Auftragsverarbeiter nach Art. 82 Abs. 1, Abs. 2 S. 2 DSGVO bei Verletzung seiner hier aufgeführten Pflichten für die beim Betroffenen eingetretenen immateriellen und materiellen Schäden. Selbst wenn der Verantwortliche an der Datenverarbeitung beteiligt und dieser für den Schaden verantwortlich ist, kann der Auftragsverarbeiter aufgrund der gesamtschuldnerischen Haftung nach Art. 82 Abs. 4 DSGVO vollumfänglich in Anspruch genommen werden. Erst nachträglich kann der Auftragsverarbeiter im Innenverhältnis vom Verantwortlichen den Anteil des Schadensersatzes zurückfordern.

Der Auftragsverarbeiter kann sich gem. Art. 82 Abs. 3, Abs. 4 DSGVO nur dann von der Haftung befreien, wenn er nachweisen kann, dass er sämtliche Verpflichtungen bei der Datenverarbeitung erfüllt hat und „in keinerlei Hinsicht […] verantwortlich ist“.

Drohende Geldbußen für Auftragsverarbeiter

Verarbeiter bzw. Dienstleister sollten die hier aufgeführten Pflichten im Rahmen der Auftragsverarbeitung also nicht auf die leichte Schulter nehmen. Denn werden diese Pflichten nicht erfüllt, drohen zusätzlich zur oben genannten Haftung je nach Art und Schwere der Pflichtverletzung und unabhängig davon ob ein Schaden eintritt, Geldbußen von bis zu 20.000.000 Euro oder im Fall eines Unternehmens von bis zu 4 % des gesamten weltweit erzielten Umsatzes des vorangegangenen Jahres – je nachdem, welcher Betrag höher ist!

Fazit: Solide schriftliche Vereinbarungen helfen

Mit der DSGVO kommen auf Auftragsverarbeiter zahlreiche neue Pflichten zu. Wer jedoch als Dienstleister gegenüber dem Auftraggeber bzw. Verantwortlichen auf einem korrekten Auftragsverarbeitungs-Vertrag besteht, ist schon einen großen Schritt weiter.