Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

# Auftragsverarbeitung nach DS-GVO

**- Stand: 25. Mai 2018 -**

**Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit**
**Baden-Württemberg**
**Königstraße 10a**
**70173 Stuttgart**
**Telefon 0711/615541-0**
**Telefax 0711/615541-15**
**E-Mail: *poststelle@lfdi.bwl.de***
**(Schutzbedürftige Daten sollten nicht unverschlüsselt per E-Mail oder via Telefax übertragen werden.)**
**PGP-Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962**
**Homepage: www.baden-wuerttemberg.datenschutz.de**

**1.) Allgemeines**
Nach der EU-DSGVO ist für die **Auftragsverarbeitung kennzeichnend**, dass

- der Auftragsverarbeiter über die bloße Beauftragung hinaus gegenüber dem Verantwortlichen **weisungsabhängig** ist, selbst wenn der Auftragsverarbeiter über ein umfassenderes Know-how als sein Auftraggeber verfügt und einen gewissen Spielraum für selbständige Entscheidungen hat, und
- der Auftragsverarbeiter vom Verantwortlichen **überwacht** wird.

**2.) Auswahl des Auftragsverarbeiters**

Verantwortliche dürfen nur Auftragsverarbeiter einsetzen, die eine **hinreichende Garantie für eine datenschutzkonforme Datenverarbeitung**, insbesondere dass der Schutz der Rechte der betroffenen Personen gewährleistet ist, bieten (vgl. Art. 28 Abs. 1 EU-DSGVO; Erwägungsgrund 81 Satz 1; § 62 Abs. 2 BDSG-neu). Der **Nachweis** für diese Qualifikation kann über entsprechende **Zertifizierungen** gemäß Art. 42 EU-DSGVO und anerkannte Verhaltenskodizes nach Art. 40 EU-DSGVO geführt werden (Art. 28 Abs. 5 EU-DSGVO).

**3.) Auftragsverarbeitungsverhältnis**

Die Auftragsverarbeitung darf nur auf der Grundlage eines **bindenden Vertrages** zwischen dem Verantwortlichen und dem Auftragsverarbeiter erfolgen. In diesem müssen Gegenstand und Verarbeitungsdauer, sowie die Art und der Zweck der Datenverarbeitung, die Art der zu verarbeitenden personenbezogenen Daten, die Kategorie der betroffenen Personen und die Rechte und Pflichten des Verantwortlichen und des Auftragsverarbeiters festgelegt werden (Art. 28 Abs. 3 EU-DGSVO; vgl. § 62 Abs. 5 DSAnpUG-EU).

Art. 28 Abs. 3 und 6 EU-DSGVO sieht vor, dass auch „**ein anderes Rechtsinstrument**“ als ein eigens ausgehandelter Vertrag nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten Basis der Auftragsdatenverarbeitung sein kann.

Die Auftraggeber bzw. Auftragnehmer haben somit die Auswahl zwischen

- individuellen Verträgen,
- Standardverträgen, die die EU-Kommission bereitstellt,
- Standardverträgen, die die Aufsichtsbehörde bereitstellt, und
- zertifizierten Vertragsmustern.

Der ADV-Vertrag muss nach Art. 28 Abs. 9 EU-DSGVO entweder **schriftlich** oder „**in einem elektronischen Format**“ abgefasst sein (vgl. § 62 Abs. 6 BDSG-neu). Dabei genügt nicht jede bestätigende E-Mail. Vielmehr sind nur solche elektronische Formate akzeptabel, die beiden Parteien zu ihrer Information zugänglich sind, und wenn damit dokumentiert ist, welcher Vertragsinhalt bestätigt wurde, was durchaus auch durch entsprechendes Setzen eines Häkchens erfolgen kann.

## 4.) Pflichten des Verantwortlichen

Der **Verantwortliche** ist grundsätzlich für jedwede Verarbeitung personenbezogener Daten, die er selbst vornimmt oder von ihm durch einen Auftragsverarbeiter veranlasst wird, verantwortlich (Art. 24, Art. 4 Nrn. 2, 7 und 8 EU-DSGVO, Erwägungsgrund 74 S. 1; § 62 Abs. 1 BDSG-neu).

Der Verantwortliche hat die **Gewährleistung der in Kapitel III der EU-DSGVO** aufgeführten Betroffenenrechte (Informationspflichten, Auskunftsansprüche, Recht auf Löschung und Berichtigung, Recht auf Einschränkung der Verarbeitung, Recht auf Datenübertragbarkeit, Widerspruchsrecht) sicherzustellen. Dabei er den betroffenen Personen nach Art. 13 Abs. 1 lit. e) und f), Abs. 3, Art. 14 Abs. 1 lit. e) und f), Abs. 4, Art. 15 Abs. 1 lit. c EU-DSGVO auch mitteilen, dass Auftragsverarbeiter als Empfänger ihrer Daten in Betracht kommen und ob die Daten in Drittländern bzw. zu einem anderen Zweck als zum Zeitpunkt ihrer Erhebung von diesen verarbeitet werden. Diese Rechte hat die betroffene Person gegenüber dem Verantwortlichen geltend zu machen (vgl. § 62 Abs. 1 BDSG-neu). Der Verantwortliche muss darüber zu befinden, wie er den Ansprüchen der betroffenen Personen gerecht wird. Die Durchführung der dafür erforderlichen technischen und organisatorischen Maßnahmen kann er dem Auftragsverarbeiter vertraglich überlassen. Auch muss der Verantwortliche nach Art. 19 EU-DSGVO den Auftragsverarbeiter als Empfänger von Daten unterrichten, wenn diese berichtigt oder gelöscht wurden bzw. wenn deren Verarbeitung nach Art. 18 EU-DSGVO einzuschränken ist.

Der Verantwortliche ist nach Art. 32 Abs. 1 EU-DSGVO verpflichtet, dafür Sorge zu tragen, dass der Auftragsverarbeiter entsprechend dem **Stand der Technik** die erforderlichen **technischen und organisatorischen Maßnahmen** zum Schutz der personenbezogenen Daten und für die rechtmäßige Datenverarbeitung der von ihm verarbeiteten Daten trifft. Der Verantwortliche muss diese in dem AV-Vertrag mit dem Auftragsverarbeiter vereinbaren. Aus Art. 32 Abs. 1 EU-DSGVO ergeben sich dazu Mindestanforderungen wie Pseudonymisierung, Verschlüsselung und Maßnahmen zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Hinzu kommen technische und organisatorische Maßnahmen zur schnellen Wiederherstellung von Systemen bei technischen Zwischenfällen (Art. 32 Abs. 1 lit. c) EU-DSGVO) und solche zur regelmäßigen Evaluierung der Wirksamkeit aller technisch-organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d) EU-DSGVO; vgl. § 64 Abs. 2 und 3 DSAnpUG-EU ).

Ferner muss der Verantwortliche nach Art. 33 und 34 EU-DSGVO die Aufsichtsbehörde und ggf. die betroffene Person von **Datenschutzverletzungen**, auch wenn sie sich beim Auftragsverarbeiter ereignet haben, unterrichten (vgl. § 66 BDSG-neu).

Zwar ist nur der Verantwortliche verpflichtet, u. U. eine **Datenschutzfolgenabschätzung** nach Art. 35 f. EU-DSGVO, § 67 BDSG-neu durchzuführen, wenn die Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt. Doch muss dabei auch in die Bewertung miteinbezogen werden, dass ein Auftragsverarbeiter eingesetzt wird, welche Risiken damit verbunden sind und welche Garantien es gibt, diese zu minimieren, wobei die Sicherheitskonzeption des Auftragsverarbeiters zu berücksichtigen ist. Insbesondere ist von Bedeutung, ob Auftragsverarbeiter betraut werden, die die Daten im „unsicheren“ Ausland verarbeiten.

Schließlich ist es Aufgabe des Verantwortlichen, gemeinsam mit dem Auftragsverarbeiter dafür Sorge zu tragen, dass bei der Datenübermittlung an Empfänger in Drittländern die Grundsätze des Kapitels V der EU-DSGVO eingehalten werden.

## 5.) Weisungsrecht und Kontrollpflicht des Verantwortlichen

Der Verantwortliche hat den Auftragsverarbeiter grundsätzlich fortwährend zu **kontrollieren**, ob dieser die Einhaltung der Datenschutzvorschriften gewährleisten kann. Auch wenn der Auftragsverarbeiter seine Befähigung und Zuverlässigkeit durch ein Zertifikat i. S. der EU-DSGVO nachgewiesen hat, bleibt der Verantwortliche nach Art. 42 Abs. 2 EU-DSGVO neben dem Auftragsverarbeiter für die generelle Einhaltung der Datenschutzvorschriften verantwortlich. Er kann sich aber auf das Zertifikat, soweit dessen Garantie geht, maximal für die Dauer von drei Jahren verlassen (Art. 42 Abs. 7 DSGVO). Allerdings schließt die EU-DSGVO nicht aus, dass der Verantwortliche mit dieser Aufgabe einen **fachkundigen Dritten** beauftragt.

Nach Art. 29 EU-DSGVO ist der Verantwortliche berechtigt und verpflichtet, dem Auftragsverarbeiter **Weisungen** zu erteilen, soweit diese zur Durchsetzung des AV-Vertrags oder der gesetzlichen Pflichten des Verantwortlichen bzw. des Auftragsverarbeiters erforderlich sind. Diese können im Einzelfall oder generell erfolgen. Auch mit dieser Aufgabe kann der Verantwortliche ähnlich wie bei seinen Kontrollverpflichtungen einen fachkundigen Dritten betrauen.

## 6.) Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter muss

- den rechtmäßig erteilten **Weisungen** des Auftraggebers **Folge leisten** (Art. 29 EU-DSGVO),

- nach Art. 32 Abs. 1 und 2 EU-DSGVO, § 64 BDSG-neu entsprechend dem Stand der Technik **technische und organisatorische Maßnahmen** für ein angemessenes Schutzniveau der personenbezogenen Daten ergreifen. Dazu gehören insbesondere:

  - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenverarbeitung auf Dauer sicherzustellen,
  - die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
  - die Fähigkeit, die Verfügbarkeit der Daten und den Zugang zu ihnen bei einem Zwischenfall rasch wiederherzustellen, und
  - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zu installieren.

- die **Verletzung des Schutzes personenbezogener Daten** nach Art. 33 Abs. 2 EU-DSGVO unverzüglich dem Verantwortlichen **melden**,

- nach Art. 37 Abs. 1 EU-DSGVO einen **betrieblichen Datenschutzbeauftragten** insbesondere dann bestellen, wenn die Kerntätigkeit des Auftragsverarbeiters in der Durchführung von Datenverarbeitungen besteht, die eine umfangreiche regelmäßige und systematische Überwachung des Personals erforderlich macht,

- Kontrollen durch den Auftraggeber **ermöglichen** und in angemessener Weise daran mitwirken,

- gewährleisten, dass nur **Mitarbeiter** mit der Datenverarbeitung betraut werden, die sich **verpflichtet** haben, das **Datenschutzrecht** einzuhalten,

- den **Verantwortlichen** bei der Erfüllung seiner datenschutzrechtlichen Verpflichtungen nach Kapitel III EU-DSGVO technisch und organisatorisch **unterstützen** bzw. den im AV-Vertrag vom Auftragsverarbeiter **übernommenen Verpflichtungen** – z. B. der betroffenen Person Auskünfte nach Art. 15 EU-DSGVO zu erteilen – entsprechen, und

- ein Verzeichnis über die von ihm übernommenen Datenverarbeitungen nach Maßgabe des Art. 30 EU-DSGVO zu führen.

**7.) Unteraufträge**

In Art. 28 Abs. 2 Satz 1 EU-DSGVO ist geregelt, unter welchen Voraussetzungen der Auftragsverarbeiter **Unterauftragnehmer** einschalten darf, nämlich wenn er dafür die Genehmigung aller in der Verarbeitungskette vor ihm Kommenden hat (vgl. § 62 Abs. 3 DSAnpUG-EU).

Für die Zulässigkeit der Einschaltung von Unterauftragnehmern bedarf es im Vorhinein einer **schriftlichen Genehmigung** des Verantwortlichen, die auch in elektronischer Form erteilt werden kann. Zwar ist die letztgenannte Form in Art. 28 Abs. 2 EU-DSGVO nicht ausdrücklich erwähnt, doch können für eine solche Genehmigung keine weitergehenden Anforderungen als für den AV-Vertrag selbst verlangt werden, zumal es möglich ist, die Zustimmung zur Unterbeauftragung bereits in diesem zu erteilen.

Ist dem Auftragsverarbeiter die Vergabe von Unteraufträgen aufgrund einer **allgemeinen schriftlichen Genehmigung** gestattet, muss er den Verantwortlichen vom Gebrauchmachen von dieser Befugnis sowie von jeder diesbezüglichen Änderung informieren. Das kann auch elektronisch erfolgen. Dem Verantwortlichen steht jeweils ein **Einspruchsrecht** zu. (Art. 28 Abs. 2 Satz 2 EU-DSGVO). Das gilt entsprechend für spätere Veränderungen beim Einsatz von Subunternehmern.

Der Auftragsverarbeiter hat bei der Beauftragung weiterer Auftragsverarbeiter grundsätzlich **Verträge** in der Form, wie das für Auftragsverarbeitungen vorgeschrieben ist, und in der Regel mit dem **Inhalt** des Vertrages, den er selbst mit dem Verantwortlichen eingegangen ist, abzuschließen. Insbesondere muss er für hinreichende Garantien für technische und organisatorische Maßnahmen zur Sicherstellung der Datenverarbeitung entsprechend der EU-DSGVO bei dem Unterauftragsverarbeiter sorgen. Der Auftragsverarbeiter, der einen Unterauftragsverarbeiter einschaltet, hat diesem gegenüber dieselben Rechte bzw. dieselbe Verantwortung wie ein Verantwortlicher. Er muss darauf hinwirken, dass die ihm durch Vertrag mit dem Verantwortlichen auferlegten Pflichten auch von dem Unterauftragsverarbeiter eingehalten werden.

Die **Unterauftragsverarbeiter** haben grundsätzlich die gleichen **Rechte** und **Pflichten** wie ihr „Auftraggeber“.

## 8.) Auslandsbezug

Auftragsverarbeiter können nach den Vorschriften der Auftragsverarbeitung grundsätzlich sowohl im **EU-Raum** wie auch in **Drittländern** tätig werden

Der räumliche Anwendungsbereich der EU-DSGVO umfasst nach deren Art. 3 Abs. 1 alle Datenverarbeitungsvorgänge, die in der EU erfolgen, und die von einem Verantwortlichen oder einem Auftragsverarbeiter mit Hauptsitz oder einer Niederlassung in der EU veranlasst werden, unabhängig davon, wo die Datenverarbeitung konkret erfolgt. Die Regelungen der EU-DSGVO finden ferner unter bestimmten Voraussetzungen Anwendung, wenn zwar der Verantwortliche oder der Auftragsverarbeiter

nicht in der EU ansässig ist, aber die betroffene Person sich in der EU befindet (Art. 3 Abs. 2 EU-DSGVO, Marktortprinzip).

Die Weitergabe von personenbezogenen Daten an Auftragsverarbeiter in ein Land außerhalb der EU ist nach der EU-DSGVO grundsätzlich zulässig. Zu beachten sind dabei aber insbesondere die zusätzlichen Anforderungen an die **Sicherstellung des Datenschutzniveaus** beim Auftragsverarbeiter nach Kapitel V der EU-DSGVO. So muss gemäß Art. 28 Abs. 1, Art. 44 EU-DSGVO den Anforderungen der Art. 45 ff. EU-DSGVO auch im Ausland Rechnung getragen werden. Dies gilt auch bei einer Weiterübermittlung der personenbezogenen Daten durch die empfangende Stelle im Drittland (Art. 44 S. 1 2. HS EU-DSGVO; siehe auch Erwägungsgrund 101).

Die EU-DSGVO sieht für die Zulässigkeit des Datentransfers an Auftragsverarbeiter in Drittländern folgende Möglichkeiten vor:

- Feststellung der Angemessenheit des Datenschutzniveaus im Drittland durch die EU-Kommission (Art. 45 EU-DSGVO). Problematisch ist, ob US-Unternehmen, die sich dem Selbstzertifizierungssystem des Privacy Shields angeschlossen haben, ein derartiges Datenschutzniveau bieten,
- Verwendung von Standardvertragsklauseln (Art. 46 DS-GVO),
- Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules, Art. 46 Abs. 2 lit. b), Art. 47 EU-DSGVO),
- Standarddatenschutzklauseln der Kommission oder einer Aufsichtsbehörde (Art. 46 Abs. 2 lit. c) und d) EU-DSGVO),
- Genehmigte Verhaltensregeln und genehmigter Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. e) und f) EU-DSGVO),
- Datenweitergabe auf Grundlage von branchenspezifischen Verhaltensregeln gemäß Art. 40 EU-DSGVO (CoC),
- Weitergabe aufgrund von Zertifizierungen nach Art. 42 EU-DSGVO,
- einzeln ausgehandelte Vertragsklauseln (Art. 46 Abs. 3 EU-DSGVO) und
- Einwilligungen der betroffenen Person (Art. 49 Abs. 1 Abs. 1 lit. a) EU-DSGVO).