

Auftragsverarbeitung (früher Auftragsdatenverarbeitung), Art. 28 DSGVO

Für die Fortgeltung der alten Verträge über die Auftragsdatenverarbeitung ist Folgendes festzustellen:

Die meisten Altverträge, insbesondere diejenigen aus der neueren Zeit gehen bereits über die alte Rechtsgrundlage hinaus. Deshalb kann ein pauschales Urteil über die Gültigkeit von Altverträgen nicht gegeben werden. Es in jedem Einzelfall zu prüfen, ob diese auch dem neuen Recht standhalten. Verträge, die überwiegend nach Bundesdatenschutzgesetz (BDSG) ausgerichtet worden waren, werden in der Regel bereits Regelungen aller aufgelisteten Punkte enthalten. Damit die Zulässigkeit der Datenverarbeitung nicht unnötig gefährdet wird – die Rechtsfolge kann die Ungültigkeit des bisherigen Vertrages und daher dann auch die rechtsunsichere bis rechtswidrige weitere Datenverarbeitung sein –, sollte in jedem Zweifel die Auftragsverarbeitung neu verhandelt werden.

Eine Musterauftragsverarbeitung, die gut übernommen werden kann, ist https://www.lda.bayern.de/media/muster_adv.pdf.

Auftragsverarbeiter ist nach Art. 4 Nr. 8 DSGVO eine Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Verantwortlicher ist dabei gemäß Art. 4 Nr. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen über die Mittel und Zwecke der Verarbeitung personenbezogener Daten entscheidet. Hierbei kommt es maßgeblich auf die Entscheidung über die Verarbeitungszwecke an, während die Entscheidung über die technisch-organisatorischen Fragen der Verarbeitung auch auf den Auftragsverarbeiter delegiert werden kann.

Insgesamt legt die DSGVO den Auftragsverarbeitern künftig mehr Verantwortung und mehr Pflichten auf.

Gemäß Art. 28 Abs. 1 DSGVO wird dem Verantwortlichen vor der Auftragsvergabe zunächst eine Prüfung der Geeignetheit des Auftragsverarbeiters auferlegt. Der Verantwortliche darf sich danach nur solcher Auftragsverarbeiter bedienen, die hinreichende Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz anwenden, so dass die Verarbeitung im Einklang mit der DSGVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Zum Beleg solcher Garantien können auch genehmigte Verhaltensregeln des Auftragsverarbeiters nach Art. 40 DSGVO oder Zertifizierungen nach Art. 42 DSGVO als Tatsachen herangezogen werden.

Der Pflichtinhalt eines Auftragsverarbeitervertrages gemäß Art. 28 DSGVO ist der Folgende:

• Gegenstand und Dauer der Datenverarbeitung
• Art und Zweck der Verarbeitung
• Art der personenbezogenen Daten
• Kategorien betroffener Personen
• Pflichten und Rechte des Verantwortlichen
• Verpflichtung auf Verarbeitung nur aufgrund dokumentierter Weisung
• Verpflichtung zur Vertraulichkeit

• Verpflichtung, dass der Auftragsverarbeiter alle nach Art. 32 DSGVO erforderlichen Maßnahmen zur Sicherheit der Verarbeitung ergreift
• Verpflichtung des Auftragsverarbeiters, die Bedingungen zur Beauftragung von weiteren Auftragsverarbeitern einzuhalten, Art. 28 Abs. 2 und 4 DSGVO
• Unterstützungspflichten des Auftragsverarbeiters mit geeigneten technischen und organisatorischen Maßnahmen bei Betroffenenrechten/Anfragen und Ansprüchen Betroffener
• Unterstützungspflicht des Auftragsverarbeiters bei Sicherheit der Verarbeitung bei Meldungen von Datenschutzverstößen, bei der Datenschutzfolgeabschätzung und bei der vorherigen Konstellation einer Aufsichtsbehörde
• Löschung bzw. Rückgabeverpflichtung des Auftragsverarbeiters nach Beendigung des Auftrags
• Pflicht des Auftragsverarbeiters, Information zur Verfügung zu stellen und Ermöglichung von Kontrollen

Bitte beachten Sie, dass nach neuem Recht gemäß Art. 30 Abs. 2 DSGVO jeder Auftragsverarbeiter eine Übersicht von Verarbeitungstätigkeiten zu führen hat; vgl. das Muster auf diesen Seiten.