DIGITALISIERUNGSTIPP

Auftragsverarbeitung nach Art. 28 DSGVO

Auftragsverarbeitung

Art. 4 Nr. 8 DSGVO definiert den Auftragsverarbeiter als „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Kennzeichnend ist, dass der Auftragsverarbeiter für den Verantwortlichen tätig wird, also für dessen Zwecke Daten verarbeitet. Der Auftragsverarbeiter ist gegenüber dem Verantwortlichen weisungsgebunden. Er darf die Daten nur nach dem Willen des Verantwortlichen verarbeiten. Die technische Umsetzung, also die Wahl von Hard- und Software, kann dabei dem Auftragsverarbeiter übertragen werden.

Werden personenbezogene Daten verarbeitet, trägt der Verantwortliche, also die Person oder das Unternehmen, welche über die Zwecke und Mittel der Verarbeitung entscheidet, die Verantwortung dafür. Doch nicht in allen Fällen verarbeitet der Verantwortliche die personenbezogenen Daten selbst. Oft ist die Datenverarbeitung komplex und aufwendig und wird daher ausgelagert. Möglich wird dies durch die Auftragsverarbeitung der Art. 28 ff. DSGVO.

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Alleinige Verantwortung oder Joint Control?

Die DSGVO kennt eine Joint Control, also eine gemeinsame Verantwortlichkeit, und regelt sie in Art. 26 DSGVO. Hier tragen mehrere Personen die Verantwortung und entscheiden gemeinsam über die Zwecke und Mittel der Datenverarbeitung. Die Auftragsverarbeitung ist jedoch **kein** Fall der gemeinsamen Verantwortlichkeit. Die Auftragsverarbeitung besitzt eine hierarchische Struktur und gerade keine gleichberechtigte gemeinsame Verantwortung. Wie bereits beschrieben, entscheidet bei der Auftragsverarbeitung allein der Auftraggeber über die Zwecke und Mittel der Datenverarbeitung und trägt daher auch die alleinige Verantwortung.

Eine Ausnahme von der Verantwortlichkeit des Auftraggebers ist der sog. Aufgaben- oder Funktionsexzess des Auftragsverarbeiters. Dabei überschreitet er die ihm zugewiesenen Kompetenzen indem er etwa Daten des Auftraggebers für eigene Zwecke oder Zwecke Dritter verarbeitet und somit gegen die DSGVO verstößt. Art. 28 Abs. 10 DSGVO macht den Auftragsverarbeiter dann zum Verantwortlichen im Sinne der DSGVO, sodass er für die Verarbeitungsvorgänge haftbar gemacht werden kann und so eine Haftung des ursprünglichen Auftraggebers entfällt.

Auswahl des Auftragsverarbeiters

Da der Verantwortliche seine Verantwortung nicht an den Auftragsverarbeiter überträgt, ist die richtige Wahl des Auftragsverarbeiters wichtig. Daher besagt Art. 28 Abs. 1 DSGVO auch, dass der Verantwortliche nur mit Auftragsverarbeitern zusammenarbeiten darf, die hinreichende Garantien für eine ordnungsgemäße Verarbeitung, also eine Verarbeitung im Einklang mit der DSGVO, bieten. Anhaltspunkte dafür können etwa Fachwissen, Zuverlässigkeit, Ressourcen und die Sicherheit der Verarbeitung sein. Das Ziel muss eine rechtmäßige Datenverarbeitung und ein Schutz der Betroffenenrechte sein. Die Mittel dafür sind technische und organisatorische Maßnahmen (sog. TOMs). Beispiele für solche Maßnahmen sind etwa die Pseudonymisierung, bei welcher der Personenbezug aufgehoben und später durch den Verantwortlichen wiederhergestellt wird oder eine Rechtekonzept, wonach nur bestimmte Mitarbeiter, die besonders unterwiesen wurden, diese Daten verarbeiten dürfen; für alle anderen Mitarbeiter ist ein Zugang zu diesen Daten nicht möglich.

Rechtliches Verhältnis

Art. 28 Abs. 3 DSGVO sieht für das rechtliche Verhältnis zwischen Verantwortlichen und Auftragnehmer den Vertrag oder ein anderes Rechtsinstrument vor. Relevant ist hier nur der Vertrag. Da das „andere Rechtsinstrument“ eine Öffnung für die Mitgliedsstaaten darstellt eine eigene Form eines rechtlichen Handlungsinstrument festzulegen. Davon hat Deutschland jedoch keinen Gebrauch gemacht. Im Vertrag sind die gegenseitigen Pflichten entsprechend zu formulieren. Wichtig ist hier etwa die Weisungsgebundenheit des Auftragsverarbeiters. Dafür kann gem. Art. 28 Abs. 6 DSGVO auch auf die Standardvertragsklauseln der EU-Kommission zurückgegriffen werden. Diese sind abrufbar unter:

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0915&from=DE

Mittelstand-Digital Zentrum Chemnitz
c/o Technische Universität Chemnitz
09125 Chemnitz
0371 531-19935
info@digitalzentrum-chemnitz.de

Michael Rätze
0371 531-35860
michael.raetze@digitalzentrum-chemnitz.de

digitalzentrum-chemnitz.de