Auftragsverarbeitungsvertrag (Anlage)

Anlage zum Hauptvertrag

1. Anwendungsbereich

Bei der Erbringung der Leistungen gemäß dem Hauptvertrag verarbeitet der Auftragnehmer personenbezogene Daten, die der Auftraggeber zur Erbringung der Leistungen zur Verfügung gestellt hat und bezüglich derer der Auftraggeber als Verantwortlicher im datenschutzrechtlichen Sinn fungiert („Auftraggeber-Daten"). Diese Anlage spezifiziert die Datenschutzpflichten und -rechte der Parteien im Zusammenhang mit der Verarbeitung der Auftraggeber-Daten zur Erbringung der Leistungen nach dem Hauptvertrag.

2. Umfang der Beauftragung/Weisungsbefugnisse des Auftraggebers

2.1 Der Auftragnehmer wird die Auftraggeber-Daten ausschließlich im Auftrag und gemäß den Weisungen des Auftraggebers verarbeiten, sofern der Auftragnehmer nicht gesetzlich dazu verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2.2 Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt ausschließlich in der Art, dem Umfang und zu dem Zweck wie im Hauptvertrag zu dieser Anlage spezifiziert; die Verarbeitung betrifft ausschließlich die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen.

2.3 Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

2.4 Der Auftraggeber behält sich das Recht zur Erteilung von Weisungen über Art, Umfang, Zwecke und Mittel der Verarbeitung von Auftraggeber-Daten vor.

3. Anforderungen an Personal

3.1 Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

3.2 Der Auftragnehmer stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Auftraggeber-Daten haben, diese nur auf seine Anweisung verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

4. Sicherheit der Verarbeitung

4.1 Der Auftragnehmer ergreift alle geeigneten technischen und organisatorischen Maßnahmen, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.

4.2 Der Auftragnehmer hat vor dem Beginn der Verarbeitung der Auftraggeber-Daten insbesondere die technischen und organisatorischen Maßnahmen zu ergreifen und während des Hauptvertrags aufrechtzuerhalten sowie sicherzustellen, dass die Verarbeitung von Auftraggeber-Daten im Einklang mit diesen Maßnahmen durchgeführt wird.

5. Inanspruchnahme weiterer Auftragsverarbeiter

5.1 Der Auftraggeber genehmigt hiermit in allgemeiner Weise die Inanspruchnahme weiterer Auftragsverarbeiter durch den Auftragnehmer.

5.2 Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter informieren. Der Auftraggeber ist berechtigt, gegen jede beabsichtigte Änderung Einspruch zu erheben. Erhebt der Auftraggeber Einspruch, ist dem Auftragnehmer die beabsichtigte Änderung untersagt.

5.3 Der Auftragnehmer wird jedem weiteren Auftragsverarbeiter vertraglich dieselben Datenschutzpflichten auferlegen, die in dieser Anlage in Bezug auf den Auftragnehmer festgelegt sind.

5.4 Der Auftragnehmer wird vor jeder Beauftragung sowie regelmäßig während der Beauftragung überprüfen, dass die weiteren Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergriffen haben und diese so durchgeführt werden, dass die Verarbeitung der Auftraggeber-Daten gemäß dieser Anlage erfolgt.

6. Rechte der betroffenen Personen

6.1 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren mit technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

6.2 Der Auftragnehmer wird insbesondere:

- den Auftraggeber unverzüglich informieren, falls sich eine betroffene Person mit einem Antrag auf Wahrnehmung ihrer Rechte in Bezug auf Auftraggeber-Daten unmittelbar an den Auftragnehmer wenden sollte;
- dem Auftraggeber auf Anfrage alle bei ihm vorhandenen Informationen über die Verarbeitung von Auftraggeber-Daten geben, die der Auftraggeber zur Beantwortung des Antrags einer betroffenen Person benötigt und über die der Auftraggeber nicht selbst verfügt.

7. Sonstige Unterstützungspflichten des Auftragnehmers

7.1 Der Auftragnehmer meldet dem Auftraggeber, unverzüglich nachdem ihm eine solche bekannt geworden ist, jede Verletzung des Schutzes von Auftraggeber-Daten, insbesondere Vorkommnisse, die zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu Auftraggeber-Daten führen. Die Meldung enthält nach Möglichkeit eine Beschreibung:

- der Art der Verletzung des Schutzes der Auftraggeber-Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- der wahrscheinlichen Folgen der Verletzung des Schutzes der Auftraggeber-Daten;
- der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes der Auftraggeber-Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7.2 Für den Fall, dass der Auftraggeber verpflichtet ist, die Aufsichtsbehörden und/oder Betroffenen nach Art. 33, 34 DSGVO zu informieren, wird der Auftragnehmer den Auftraggeber auf dessen Anfrage unterstützen, diese Pflichten einzuhalten.

7.3 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren bei etwa von ihm durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

8. Datenlöschung und -zurückgabe

Der Auftragnehmer wird auf die Weisung des Auftraggebers hin mit Beendigung des Hauptvertrages alle Auftraggeber-Daten entweder vollständig und unwiderruflich löschen oder an den Auftraggeber zurückgeben, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.

9. Nachweise und Überprüfungen

9.1 Der Auftragnehmer hat sicherzustellen und regelmäßig zu kontrollieren, dass die Verarbeitung der Auftraggeber-Daten mit dieser Anlage sowie den Weisungen des Auftraggebers in Einklang steht.

9.2 Der Auftragnehmer wird die Umsetzung der Pflichten nach dieser Anlage in geeigneter Weise dokumentieren und dem Auftraggeber entsprechende Nachweise auf dessen Anfrage vorlegen. Der Auftragnehmer wird insbesondere dokumentieren:

- alle Vertraulichkeitsverpflichtungen von Personen, die Auftraggeber-Daten verarbeiten;
- alle sich in seinem Einwirkungsbereich ereignenden Verletzungen des Schutzes von Auftraggeber-Daten einschließlich aller damit im Zusammenhang stehenden Fakten, deren Auswirkungen und von ihm ergriffene Abhilfemaßnahmen;
- alle Verträge über die Inanspruchnahme weiterer Auftragsverarbeiter und alle Prüfungen weiterer Auftragsverarbeiter im Sinne von Ziffer 5.;
- alle auf Weisung des Auftraggebers erfolgten Löschungen von Auftraggeber-Daten.

9.3 Der Auftraggeber ist berechtigt, den Auftragnehmer vor dem Beginn der Verarbeitung von Auftraggeber-Daten und regelmäßig während der Laufzeit des Hauptvertrags bezüglich der Einhaltung der Regelungen dieser Anlage, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, selbst oder durch einen von ihm beauftragten Prüfer zu überprüfen; einschließlich durch Inspektionen. Der Auftragnehmer ermöglicht solche Überprüfungen und trägt durch alle zweckmäßigen und zumutbaren Maßnahmen zu solchen Überprüfungen bei, unter anderem durch:

- die Gewährung der notwendigen Zugangs- und Zugriffsrechte und
- der Bereitstellung aller notwendigen Informationen.