

1. Gegenstand des Auftrages

1.1 Diese Anlage konkretisiert die Verpflichtungen der Parteien zum Datenschutz, die sich aus der im Einzelvertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Einzelvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch vom Auftragnehmer beauftragte personenbezogene Daten („Daten“) des Auftraggebers verarbeiten

1.2 Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedstaat der europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2. Beginn und Dauer des Auftrages

Der Beginn und die Dauer des Auftrages ergeben sich aus dem Einzelvertrag.

3. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

3.1 Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten (nachfolgend zusammenfassend „Verarbeitung“) durch den Auftragnehmer für den Auftraggeber sind die im jeweiligen Einzelvertrag beschriebenen Kategorien und Arten personenbezogener Daten.

3.2 Die von der Verarbeitung der personenbezogenen Daten betroffenen Personengruppen sind im Einzelvertrag beschrieben.

4. Pflichten des Auftragnehmers

4.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern der Auftragnehmer nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4.2 Der Auftragnehmer verwendet die personenbezogenen Daten ausschließlich für die in dem Einzelvertrag genannten Zwecke und ist insbesondere nicht berechtigt, die personenbezogenen Daten an Dritte weiterzugeben. Der Auftragnehmer ist nicht berechtigt, ohne schriftliche Zustimmung des Auftraggebers Kopien der personenbezogenen Daten zu erstellen. Hiervon ausgenommen sind Sicherheitskopien, soweit diese zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, deren Aufbewahrung nach den gesetzlichen Aufbewahrungspflichten erforderlich ist.

4.3 Der Auftragnehmer wird die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt halten. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

4.4 Bei der Erfüllung der Betroffenenrechte durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen.

4.5 Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn eine vom Auftraggeber erteilte Weisung nach Meinung des Auftragnehmers gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

4.6 Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechnigte Interessen des Auftragnehmers dem nicht entgegenstehen.

4.7 Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

4.8 Der Auftraggeber ist nach vorheriger Terminvereinbarung berechtigt, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort.

4.9 Wenn und soweit die Verarbeitung von Daten durch Beschäftigte des Auftragnehmers in Privatwohnungen stattfindet, wird der Auftragnehmer durch die in Anhang 1 beschriebenen technischen und organisatorischen Maßnahmen die Sicherheit der Daten sicherstellen.

4.10 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des

Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften im eigenen Betrieb.

4.11 Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt. Die Kontaktdaten des Datenschutzbeauftragten sind in Anhang 1 aufgeführt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber mitzuteilen.

5. Rechte und Pflichten des Auftraggebers

5.1 Der Auftraggeber ist verantwortliche Stelle im Sinne von Art. 4 Nr. 7 DSGVO für die Erhebung, Verarbeitung und/oder Nutzung der personenbezogenen Daten im Auftrag durch den Auftragnehmer.

5.2 Für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

5.3 Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der bei dem Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

5.4 Der Auftraggeber informiert der Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

5.5 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

6. Weisungsbefugnisse des Auftraggebers

6.1 Der Auftraggeber hat gegenüber dem Auftragnehmer im Hinblick auf die Verarbeitung der personenbezogenen Daten ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung, das er durch Einzelweisungen konkretisieren kann.

6.2 Die Weisungen erfolgen mündlich oder schriftlich. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich bestätigen. E-Mail ist zur Wahrung des Schriftformerfordernisses nach dieser Ziffer 6.2 ausreichend.

7. Technische und organisatorische Maßnahmen

7.1 Der Auftragnehmer wird die in Anhang 1 aufgeführten technischen und organisatorischen Maßnahmen zur Datensicherheit umsetzen und zu jeder Zeit während der Laufzeit dieses Vertrages einhalten.

7.2 Der Auftragnehmer wird die getroffenen technischen und organisatorischen Maßnahmen schriftlich dokumentieren oder anderweitig nachweisen. Zu diesem Zweck kann der Auftraggeber dem Auftragnehmer unter anderem Berichte unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz) vorlegen.

7.3 Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen. Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen. Dieser Mitteilungspflicht kann der Auftragnehmer auch in Form einer Mitteilung im Kundenportal nachkommen.

7.4 Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen den Parteien abzustimmen.

7.5 Soweit die bei dem Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

7.6 Die Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

8. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

8.1 Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei dem Auftragnehmer beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.

9. Unterbeauftragung

9.1 Der Auftraggeber erteilt dem Auftragnehmer eine vorherige allgemeine schriftliche Genehmigung, Unterauftragnehmer mit der Verarbeitung personenbezogener Daten zu beauftragen.

9.1.1 Die Unterbeauftragung muss schriftlich erfolgen.

9.1.2 Der Auftragnehmer wird dem Auftraggeber bei Vertragsschluss eine Liste der Unterauftragsverarbeiter, einschließlich des Namens, der Anschrift und der Rolle eines jeden Unterauftragsverarbeiters, den der Auftragnehmer derzeit zur Unterauftragsverarbeitung einsetzt, zur Verfügung stellen.

- 9.1.3 Erfolgt eine Verarbeitung im Auftrag, so muss der Auftragnehmer darauf hinwirken, dass die ihm durch diese Vereinbarung mit dem Auftraggeber auferlegten Pflichten auch von dem Unterauftragsverarbeiter eingehalten werden. Dabei arbeitet der Auftragnehmer nur mit Unterauftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
- 9.2 Der Einsatz von Unterauftragsverarbeitern erfolgt nach eigenem Ermessen des Auftragnehmers unter der Voraussetzung, dass folgende Regelungen eingehalten werden.
- 9.2.1 Der Auftragnehmer informiert den Auftraggeber im Voraus über jegliche geplante Hinzufügungen oder Ersetzungen zu der Liste der Unterauftragsverarbeiter, einschließlich des Namens, der Anschrift und der Rolle eines jeden neuen Unterauftragsverarbeiters.
- 9.2.2 Der Auftraggeber kann derartigen Änderungen gemäß Ziffer 9.2.3 widersprechen.
- 9.2.3 Der Auftraggeber kann der Unterauftragsverarbeitung innerhalb von vierzehn (14) Werktagen nach Information durch den Auftragnehmer widersprechen, sofern ein wichtiger Grund vorliegt. Widerspricht der Auftraggeber nicht innerhalb von vierzehn (14) Werktagen, so gilt der neue Unterauftragsverarbeiter als durch den Auftraggeber genehmigt.
- 9.3 Der Auftragnehmer kann einen Unterauftragsverarbeiter ohne vorherige Mitteilung austauschen, wenn sich der Grund für den Austausch aus Sicherheits- oder anderen dringenden Gründen erforderlich ist. In diesem Fall informiert der Auftragnehmer den Auftraggeber unverzüglich über die Ernennung des neuen Unterauftragsverarbeiters. Dabei gilt Ziffer 9.2.3. entsprechend.
- 9.4 Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
- 10. Pflichten des Auftragnehmers nach Beendigung des Auftrages**
- 10.1 Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – wird der Auftragnehmer die in ihrem Besitz befindlichen Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber aushändigen oder nach vorheriger Zustimmung datenschutzgerecht vernichten. Der Auftragnehmer wird das Löschen der Daten in geeigneter Weise dokumentieren.
- 10.2 Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Daten, die dem Nachweis der Auftrages- und ordnungsgemäßen Datenverarbeitung dienen, wird der Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus - gegebenenfalls gegen gesondertes Entgelt - aufbewahren.