

Auftragsverarbeitungsvertrag

Auftragsverarbeitungsvertrag zwischen

Name / Firma

Adresse

nachfolgend „Auftraggeber“ genannt

und dem der

Name / Firma

Adresse

nachfolgend „Auftragnehmer“ genannt

1. Auftrag und Vertragslaufzeit

1.1 Gegenstand

Mit Datum vom _____ haben die Parteien einen Kooperationsvertrag (nachfolgend „Hauptvertrag“ genannt) geschlossen. Die vom Auftragnehmer zu erbringenden Leistungen ergeben sich aus Ziffer [...] des Vertrags. In diesem Zusammenhang erhebt, speichert und verarbeitet der Auftragnehmer personenbezogene Daten. Der Auftraggeber ist Verantwortlicher, der Auftragnehmer Auftragsverarbeiter hinsichtlich der zu verarbeitenden personenbezogenen Daten (nachfolgend „Daten“ genannt).

1.2 Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags. Daneben kann dieser Auftragsverarbeitungsvertrag auch separat vom Hauptvertrag mit einer Frist von einem Montag zum Monatsende gekündigt werden und durch einen neuen Vertrag ersetzt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt hiervon unberührt.

2. Auftragsinhalt

2.1 Art und Zweck der Datenverarbeitung

Durch den Arbeitnehmer erfolgt folgende Datenverarbeitung:

- Art der Verarbeitung (z.B.: elektronische Erfassung und Speicherung von Anrede, Vor- und Nachname und E-Mailadresse von Teilnehmern der Kurse des Auftraggebers sowie Speicherung auf den Servern des Auftraggebers): _____
- Zweck der Verarbeitung (z.B.: Versendung des Newsletters des Auftraggebers ca. 2 Mal pro Woche): _____

Die Durchführung der hiermit vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

2.2 Datenkategorien und betroffene Personen

2.2.1 Von der Datenverarbeitung durch den Auftragnehmer sind folgende Datenkategorien betroffen:

- ☐ Personalstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Teilnehmerhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunftsteilen, oder aus öffentlichen Verzeichnissen)
- ☐ _____

2.2.2 Die Kategorien der betroffenen Personen sind folgende:

- ☐ Teilnehmer
- ☐ Interessenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ _____

3. Technisch-organisatorische Maßnahmen

3.1 Vor Auftragsvergabe wird der Auftragnehmer den Auftraggeber über die technisch-organisatorischen Maßnahmen informieren. Diese werden durch den Auftraggeber geprüft und dem Vertrag als **Anlage** beigefügt. Ergeben sich durch die Prüfung Änderungen, wird der Auftragnehmer diese unverzüglich umsetzen.

3.2 Der Auftragnehmer hat für die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere auch im Hinblick auf Art. 5 Abs. 1, Abs. 2 DS-GVO Sorge zu tragen. Er wird die notwendigen Maßnahmen zur Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit sowie Belastbarkeit der Systeme treffen. Dabei wird der Auftragnehmer den Stand der Technik, die Implementierungskosten und Art, Umfang und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen entsprechend Art. 32 Abs. 1 DS-GVO im ausreichenden Maße zu berücksichtigen.

3.3 Der Auftragnehmer ist frei, technische und organisatorische Maßnahmen anzupassen, insbesondere alternative Mittel einzusetzen, soweit das Sicherheitsniveau dadurch nicht unterschritten wird. Bei wesentlichen Änderungen wird er dem Auftraggeber eine angepasste **Anlage** zur Verfügung stellen, welche durch die bestehende **Anlage** ersetzt wird.

4. Weisungen und Unterstützungsleistungen

4.1 Der Auftraggeber ist als Verantwortlicher „Herr der Daten“ und wird dem Auftragnehmer entsprechende Weisungen erteilen, die soweit sie mündlich ergangen sind, auf Anfrage stets nochmal in Textform erfolgen.

4.2 Entsprechend ist es dem Auftragnehmer nicht gestattet, mit den Daten eigenmächtig zu verfahren, insbesondere sie zu berichtigen oder zu löschen. Entsprechende Anfragen Dritter wird er umgehend an den Auftraggeber weiterleiten. Auskunftsverlangen oder sonstige Anfragen Dritter im Zusammenhang mit den Daten wird er nach vorheriger Absprache mit dem Auftraggeber nachkommen.

4.3 Der Auftragnehmer verfügt hinsichtlich der Daten des Auftraggebers über ein Verarbeitungsverzeichnis sowie ein Löschkonzept, das er entsprechend umsetzen wird. Der Auftragnehmer wird ferner für eine Datenportabilität der Daten Sorge tragen sowie dafür, dass sämtliche Datenprozesse dokumentiert werden.

4.4 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

4.5 Der Auftragnehmer wird den Verantwortlichen bei Ausnahmen von der Weisungspflicht unterrichten, wenn nicht einschlägige Rechtsvorschriften eine solche Mitteilung verbieten.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer wird seine Pflichten gemäß Art. 28 bis 33 DSGVO beachten. Hierzu zählt insbesondere:

- Die Bestellung eines Datenschutzbeauftragten. Seine Kontaktdaten lauten:

- Die Sicherstellung von Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer wird nur solche Mitarbeiter mit der Auftragsdurchführung betrauen, die nachweislich zur Vertraulichkeit verpflichtet wurden und im Datenschutzrecht geschult wurden. Der Auftragnehmer wird dafür Sorge tragen, dass die Mitarbeiter die Daten nur innerhalb ihrer Befugnisse, nach Weisung des Auftraggebers oder soweit anderweitig nach diesem Vertrag oder gesetzlichen Vorschriften gestattet bearbeiten.
- Die Umsetzung und Einhaltung der für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO gemäß **Anhang**.
- Die Zusammenarbeit mit dem Auftraggeber bei Anfragen und/oder Maßnahmen der Aufsichtsbehörden oder sonstiger Behörden. Der Auftragnehmer benachrichtigt den Auftraggeber umgehend, falls die Aufsichtsbehörde ihm gegenüber Kontrollen oder anderweitige Maßnahmen vornimmt bzw. ergreift.

Der Auftragnehmer unterstützt den Verantwortlichen bei der Erfüllung seiner Pflichten zu Betroffenenrechten wie folgt: _____ (z.B. durch bestimmte technisch-organisatorische Maßnahmen)

- Die regelmäßige Kontrolle der internen Prozesse und technischen und organisatorischen Maßnahmen, um eine rechtskonforme Datenverarbeitung zu gewährleisten.
- Die Dokumentation der Prozesse und insbesondere auch der technischen und organisatorischen Maßnahmen, um eine Nachweisbarkeit (Accountability) herzustellen sowie
- Die Verwendung der Daten ausschließlich für auftragsgemäße Zwecke.

6. Unterauftragsverhältnisse

6.1 Eine Unterbeauftragung liegt vor, wenn eine Dienstleistung, die sich unmittelbar auf die Erbringung der Hauptleistung bezieht, an einen Dritten delegiert wird. Hiervon nicht umfasst sind Nebenleistungen, wie z.B. Transportdienstleistungen, Wartung sowie Entsorgung von Datenträgern. Auch bei solchen Nebenleistungen hat der Auftragnehmer jedoch eine datenschutzrechtliche Konformität durch entsprechende Vereinbarungen und Kontrollen sicherzustellen.

6.2 Die Involvierung eines Unterauftragnehmers bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer bereits jetzt zu unter der Bedingung zu, dass eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zwischen Auftragnehmer und Unterauftragnehmer geschlossen wird:

Firma / Unterauftragnehmer	Anschrift / Land	Leistung

6.3 Der Auftragnehmer darf die Daten erst dann an den Unterauftragnehmer weitergeben, wenn alle Voraussetzungen für eine Unterbeauftragung vorliegen, insbesondere ein entsprechender Vertrag geschlossen wurde und der Auftragnehmer die technischen und organisatorischen Maßnahmen geprüft hat.

7. Kontrollrechte des Auftraggebers

7.1 Der Auftraggeber ist berechtigt, Überprüfungen beim Auftragnehmer durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Kosten, die dem Auftragnehmer durch die Duldung der Kontrollen entstehen, kann dieser ersetzt verlangen.

7.2 Der Auftragnehmer hat für eine solche Kontrolle die notwendigen Vorkehrungen zu treffen, die dem Auftraggeber eine Kontrolle nach Art. 28 DS-GVO ermöglichen. Hierzu zählen insbesondere eine umfangreiche Auskunftserteilung sowie der Nachweis über die technischen und organisatorischen Maßnahmen. Zu den möglichen Nachweisen zählen insbesondere

- die dokumentierte Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO; sowie
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)

8. Mitteilung von Datenschutzverstößen

Der Auftragnehmer wird den Auftraggeber bei der Beachtung der Pflichten gemäß Art. 32 bis 36 DS-GVO, insbesondere hinsichtlich der Meldung von Datenpannen sowie Datenschutz-Folgeabschätzungen unterstützen. Der Auftragnehmer wird in diesem Zusammenhang insbesondere die folgenden Maßnahmen ergreifen:

- Technische und organisatorische Maßnahmen, welche Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine unverzügliche Feststellung von relevanten Verletzungsereignissen erlauben;
- Unverzügliche Meldung von Datenschutzverletzungen wie auch nicht genau feststellbaren, aber wahrscheinlichen Datenschutzverletzungen an den Auftraggeber; sowie

Unverzügliche Zurverfügungstellung von Informationen, insbesondere bei Anfragen von Behörden oder Betroffenen.

9. Löschung und Rückgabe von Daten

9.1 Der Auftragnehmer wird zur Sicherstellung einer ordnungsgemäßen Datenverarbeitung und zur Einhaltung von gesetzlichen Aufbewahrungspflichten erforderliche Sicherheitskopien erstellen. Ansonsten verpflichtet sich der Auftragnehmer, die Daten nur zu kopieren oder zu duplizieren, soweit er vom Auftraggeber entsprechend instruiert wurde.

9.2 Nach Abschluss der vertraglich vereinbarten Arbeiten bzw. mit Ende des Hauptvertrags oder vorzeitig nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten bzw. ohne Wiederherstellungsmöglichkeit zu löschen. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist dem Auftraggeber vorzulegen.

9.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer über das Vertragsende für die Laufzeit der Aufbewahrungsfrist hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Ort, Datum

Ort, Datum

Unterschrift Auftraggeber

Unterschrift Auftragnehmer

Zur Kenntnis genommen:

Ort, Datum

Unterschrift Datenschutzbeauftragter (DSB)

Ort, Datum

Unterschrift Organisations-Leiter