Auftragsverarbeitungsvertrag

Zwischen dem Auftraggeber als Verantwortlichem gem. Art Nr. 7 DSGVO und SERVISUM (nachfolgend „Auftragnehmer“ genannt) als Auftragsverarbeiter gem. Art. 4 Nr. 8 DSGVO wird die die folgende Vereinbarung gem. Art. 28 Abs. 3 DSGVO abgeschlossen.

Auftraggeber und Auftragnehmer werden jeweils einzeln als „Partei“ und gemeinsam als „Parteien“ bezeichnet.

1. Vertragsgegenstand

Im Rahmen des zwischen den Parteien bestehenden Leistungsverhältnisses (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO mit personenbezogenen Daten umgeht, für die der Auftraggeber Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO ist (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen, Dauer der Auftragsverarbeitung

Der Auftragnehmer verarbeitet die personenbezogenen Daten während der Dauer des Hauptvertrages im Auftrag und nur nach Weisung des Auftraggebers. Art und Zweck der Verarbeitung sowie die Art der personenbezogenen Daten und die Kategorien betroffener Personen werden in **Anlage 1** festgelegt. Jede davon abweichende oder darüber hinaus gehende Verarbeitung von personenbezogenen Daten, insbesondere zu eigenen Zwecken, ist dem Auftragnehmer untersagt.

3. Weisungsrechte des Auftraggebers

3.1 Die Weisungen des Auftraggebers erfolgen grundsätzlich in Schrift- oder Textform (z.B. E-Mail). Abweichend hiervon können (fern-) mündliche Weisungen erfolgen, die im Nachgang in Schrift- bzw. Textform bestätigt werden.

3.2 Der Auftragnehmer ist verpflichtet, die Weisungen des Auftraggebers unverzüglich oder ggf. unter Einhaltung einer durch den Auftraggeber festgelegten, angemessenen Frist auszuführen und insbesondere personenbezogene Daten auf Weisung des Auftraggebers unverzüglich zu berichtigen, zu löschen oder zu sperren und dies auf Verlangen schriftlich zu bestätigen.

3.3 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag, gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen.

3.4 Der Auftragnehmer ist berechtigt, den Hauptvertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß dieser Vereinbarung betrifft, wenn der Auftraggeber auf der Erfüllung seiner Weisungen besteht, nachdem er vom Auftragnehmer darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Ziffer 3.3 verstoßen.

3.5 Soweit der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist, die personenbezogenen Daten auch ohne Weisung des Auftraggebers zu verarbeiten, teilt der Auftragnehmer dem Auftraggeber den Grund der Verarbeitung und die entsprechenden rechtlichen Anforderungen rechtzeitig vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4. Pflichten des Auftraggebers

4.1 Der Auftraggeber ist nach außen, also gegenüber Dritten und den Betroffenen, für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich.

4.2 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen (insbesondere in Bezug auf technische und organisatorische Maßnahmen der Datensicherheit) des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4.3 Soweit sich der Auftragnehmer gegen einen Anspruch auf Schadenersatz nach Art. 82 DSGVO, gegen ein drohendes oder bereits verhängtes Bußgeld nach Art. 83 DSGVO oder sonstige Sanktionen im Sinne des Art. 84 DSGVO mit rechtlichen Mitteln verteidigen will, erlaubt der Auftraggeber dem Auftragnehmer Details der Auftragsverarbeitung inklusive erlassener Weisungen zum Zweck der Verteidigung offenzulegen.

5. Pflichten des Auftragnehmers

5.1 Soweit sich eine betroffene Person in Wahrnehmung ihrer Rechte aus Kapitel 3 DSGVO (Art. 12 bis 23 DSGVO) unter Berücksichtigung von Teil 2, Kapitel 2 BDSG (§§ 32 bis 37 BDSG) unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer unterstützt den Auftraggeber auf zumutbare Weise mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung solcher Anträge auf Wahrnehmung der in Kapitel 3 DSGVO benannten Rechte der betroffenen Person nachzukommen.

...

5.2 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten.

5.3 Wenn dem Auftragnehmer hinsichtlich der verarbeiteten Auftraggeber-Daten eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO bekannt wird („Datenschutzvorfall"), meldet er dies dem Verantwortlichen unverzüglich. Im Rahmen der Meldung gem. Art. 33 Abs. 2 DSGVO teilt der Auftragnehmer dem Auftraggeber nach Möglichkeit den Zeitpunkt sowie Art und Ausmaß des Vorfalls, das betroffene IT-System, die betroffenen Personen, den Zeitpunkt der Entdeckung, alle denkbaren nachteiligen Folgen des Datensicherheitsvorfalls sowie die daraufhin ergriffenen Maßnahmen mit.

5.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn Rechte des Auftraggebers an den personenbezogenen Daten beim Auftragnehmer durch Maßnahmen Dritter oder durch sonstige Ereignisse maßgeblich berührt werden.

5.5 Der Auftragnehmer ist verpflichtet, auf Verlangen des Auftraggebers sämtliche Auftraggeber-Daten herauszugeben. Vom Auftraggeber erhaltene Datenträger sind gesondert zu kennzeichnen und laufend zu verwalten. Kopien und Duplikate der personenbezogenen Daten dürfen ausschließlich nach vorheriger Zustimmung durch den Auftraggeber angefertigt werden, sofern sie nicht zur ordnungsgemäßen Durchführung dieser Vereinbarung bzw. des jeweiligen Projektauftrags oder zur Einhaltung von gesetzlichen Aufbewahrungspflichten dienen.

6. Sicherheit der Verarbeitung

6.1 Der Auftragnehmer ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen insbesondere die Fähigkeit ein, die Vertraulichkeit, die Integrität, die Verfügbarkeit sowie der Belastbarkeit der Systeme auf Dauer sicherzustellen und die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Der Auftragnehmer führt regelmäßig eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durch und dokumentiert die Ergebnisse.

6.2 Der Auftragnehmer garantiert, dass er vor Beginn der Verarbeitung der Auftraggeber-Daten die in **Anlage 2** dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen implementiert, während der Dauer der Verarbeitung aufrechterhält und wenn erforderlich dem Stand der Technik und dem Risiko der Verarbeitung anpassen wird.

6.3. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7. Kontrollrechte des Auftraggebers

7.1 Der Auftragnehmer räumt dem Auftraggeber ein Kontrollrecht zur Prüfung der Datenverarbeitung sowie Einhaltung dieses Vertrags bzw. des jeweiligen Projektauftrags ein. Insbesondere stellt der Auftragnehmer dem Auftraggeber alle Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung und ermöglicht die Durchführung von Überprüfungen einschließlich Inspektionen. Die Kontrollhandlungen können ebenfalls durch einen zur Geheimhaltung verpflichteten Dritten vorgenommen werden, sofern es sich bei dem Dritten um keinen Konkurrenten des Auftragnehmers handelt.

7.2 Die Parteien sind sich einig, dass der Auftraggeber eine Überprüfung nach Ziffer 7.1 durchführt, indem er den Auftragnehmer anweist, nach seiner Wahl ein geeignetes Testat, einen Bericht oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Informationssicherheitsbeauftragter, Datenschutzauditor oder Qualitätsauditor) oder eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit – z.B. nach ISO 27001 oder BSI-Grundschutz – („Prüfungsbericht") vorzulegen. In begründeten Ausnahmen kann der Auftraggeber eigenständige Inspektionen durchführen.

7.3 Der Auftragnehmer verpflichtet sich, die Durchführung der Kontrollen zu unterstützen. Dies beinhaltet die Gewährung sämtlicher benötigter Zugangs-, Auskunfts- und Einsichtsrechte. Gleiches gilt für öffentliche Kontrollen durch die zuständige Aufsichtsbehörde gemäß den anwendbaren Datenschutzvorschriften.

7.4 Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens vier Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.

8. Unterauftragsverhältnisse

8.1 Der Auftragnehmer darf Unterauftragsverhältnisse mit weiteren Auftragsverarbeitern (Subdienstleister) begründen. Zurzeit beschäftigt der Auftragnehmer die in Anlage 3 bezeichneten Subdienstleister. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subdienstleistern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen innerhalb von zwei Wochen Einspruch zu erheben, wobei dies nicht ohne wichtigen datenschutzrechtlichen Grund erfolgen darf. Sofern der Auftraggeber keine begründeten Einwände innerhalb von 2 Wochen ab Mitteilung über die Änderung erhebt, gilt diese als durch den Auftraggeber genehmigt. Der Auftragnehmer weist den Auftraggeber bei Beginn der Frist auf diese Bedeutung seines Verhaltens hin. Im Fall eines Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder – sofern die Erbringung der Leistung ohne die beabsichtige Änderung für den Auftragnehmer nicht zumutbar ist – die Leistung gegenüber dem Auftraggeber innerhalb von zwei Wochen nach Zugang des Einspruchs einstellen und den Hauptvertrag fristlos und mit sofortiger Wirkung kündigen.

...

8.2 Ist die Beauftragung eines Subdienstleisters mit einer Übermittlung der Auftraggeber-Daten in ein Land außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraum (EWR) („Drittland“) verbunden, gelten zusätzlich die Vorgaben aus Ziffer 9.

8.3 Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Datenschutzpflichten, auch gegenüber dem Subdienstleister gelten und diesen gem. Art. 28 Abs. 4 DSGVO vor Aufnahme der Tätigkeiten entsprechend im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats zu verpflichten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

9. Übermittlung von Auftraggeber-Daten an Drittländer

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Jede Übermittlung der Auftraggeber-Daten in ein Land außerhalb von EU/EWR („Drittland“) erfolgt nur wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

10. Rückgabe und Löschung von Auftraggeber-Daten

10.1 Der Auftragnehmer hat sämtliche Auftraggeber-Daten nach Abschluss der Erbringung der Verarbeitungsleistungen und insbesondere nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Hauptvertrags) an den Auftraggeber herauszugeben und anschließend datenschutzgerecht zu löschen (inkl. vorhandener Kopien). Von dem Auftraggeber erhaltene Datenträger sind an den Auftraggeber zurückzugeben oder unter Einhaltung einer angemessenen Schutzstufe zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Dies gilt nicht, sofern nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

10.2 Dokumentationen und Protokolle, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11. Laufzeit und Kündigung

Die Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

12. Vorrangklausel

Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrages. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

Anlage 1: Art und Zweck der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen

Art und Zweck der Datenverarbeitung:
Die SERVISUM Konsular & Visum Agentur GmbH nutzt zur Auftragsabwicklung eine Kundendatenbank. Die Daten werden zur Visabeschaffung oder Legalisation gespeichert, verwendet und übermittelt.

Kategorien der personenbezogenen Daten:
Reisepass, Foto, Angaben für Visumsantrag, Ggf. weitere Anlagen zum Visumsantrag, Dokumente

Kategorien betroffener Personen:
Beschäftigte oder Mitglieder des Auftraggebers

Anlage 2: Technische und organisatorische Maßnahmen

1 Zutrittskontrolle

Gewährleistungsziel: Verwehrung des Zutritts zu Verarbeitungsanlagen, mit denen die Datenverarbeitung durchgeführt wird, für Unbefugte.

Getroffene Maßnahmen:

1.1 Die Datenverarbeitungs- und Erfassungsanlagen befinden sich ausschließlich in nicht öffentlichen Räumen. Der Zugang ist nur Mitarbeitern gestattet. Außerhalb der Bürozeiten werden die Räume durch eine Alarmanlage gesichert, die im Alarmfall die örtliche Polizei benachrichtigt.

2 Zugangskontrolle

Gewährleistungsziel: Verwehrung des Zugangs zu Datenverarbeitungssystemen, mit denen die Datenverarbeitung durchgeführt wird, für Unbefugte.

Getroffene Maßnahmen:

2.1. Der Zugang zu Datenverarbeitungssystemen ist nur durch Authentifizierung möglich, wenigstens durch ein System mit Benutzernamen und Passwort.

2.2.Weiterführende Berechtigung zur statistischen Auswertung ist nur besonders autorisierten Beschäftigten vorbehalten

3 Benutzerkontrolle

Gewährleistungsziel: Abwehr von äußeren Zugriffen auf unsere Datenbank

Getroffene Maßnahmen:

3.1. Unsere Auftragsverwaltung nutzt das Betriebssystem OS2 von IBM. Damit ist ein externes Eindringen in hohem Maße verhindert.

3.2. Dadurch, dass unsere Datenverarbeitungssysteme im Normalbetrieb offline sind (d.h. keine Verbindung zum internet haben) ist ein Datenabgriff durch unbefugte Benutzer unmöglich.

4 Übertragungskontrolle

Gewährleistungsziel: Abwehr von unbefugten Datenabgriffen bei Datenübertragungen

Getroffene Maßnahmen:

4.1. Durch technische Maßnahmen werden die Daten gegen Zugriffe auf Netzwerkebene geschützt und Schnittstellen gegen unbefugten Datenexport gesichert.

4.2. Zur Datenübertragung werden neueste Verschlüsselungstechniken genutzt.

5 Eingabekontrolle

Gewährleistungsziel: Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit und von wem eingegeben und verändert worden sind.

Getroffene Maßnahmen:

5.1. Sämtliche Eingaben und Änderungen werden mit Benutzernamen und Eingabezeit automatisch protokolliert.

6 Datenintegrität

Gewährleistungsziel: Gewährleistung, dass gespeicherte Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Getroffene Maßnahmen:

6.1. Es erfolgt die Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen und Transaktionshistorien sowie Dokumentation von Syntax von Daten.

6.2. Es bestehen Reperaturstrategien und Ausweichprozesse.

6.3. Schreib- und Änderungsrechte sind eingeschränkt.

7 Verfügbarkeitskontrolle

Gewährleistungsziel: Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Getroffene Maßnahmen:

7.1. Der gesamte Energieverbrauch der Server wird über unterbrechungsfreie Stromversorgung (USV) sichergestellt. Im Falle eines Stromausfalls garantiert die USV eine unterbrechungsfreie Umschaltung auf eine Batterieversorgung. Damit kann ein kontrolliertes Herunterfahren des Systems garantiert und Datenverlust verhindert werden.

8 Wiederherstellbarkeit

Gewährleistungsziel: Gewährleistung, dass das eingesetzte System im Störungsfall wiederhergestellt werden kann.

Getroffene Maßnahmen:

8.1. Das eingesetzte System ist technisch redundant vorhanden. Der Datenbestand unterliegt einer regelmäßigen Sicherung.

9 Prüfung, Bewertung, Evaluierung

Gewährleistungsziel: Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung.

Getroffene Maßnahmen:

9.1. Datenschutz-Management

9.2.Regelmäßige Schulung der Beschäftigten

9.3. Der Auftragsverarbeiter setzt einen langjährig und dauerhaft beschäftigten Dienstleister mit Erfahrung und Expertise zu Betreuung seinen Datenverarbeitungsanlagen ein.

Anlage 3: Unterauftragnehmer

Name	Anschrift/Land	Auftragsinhalt