Zusatzvereinbarung zur Auftragsverarbeitung

Die Parteien

asello GmbH
Technopark Raaba
Dietrich-Keller-Straße 20 6. OG West
8074 Raaba-Grambach
vertreten durch den Geschäftsführer Bernhard Schille

-- nachfolgend Auftragnehmer --

und

_____

_____

_____

_____

_____

-- nachfolgend Auftraggeber --

schließen eine Zusatzvereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO zu den Verträgen des Auftraggebers mit dem Auftragnehmer unter der Kundennunmmer _____

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem Hauptvertrag (Angebot / Leistungsbeschreibung und der AGB [https://asello.eu/agb/]) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrags.

§ 1 Gegenstand der Vereinbarung

1.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst den Betrieb der unter https://asello.eu aufgelisteten Softwarelösungen, die Speicherung von Daten sowie Dienstleistungen, die in einem individuellen Vertrag festgehalten werden. Der Auftrag umfasst alle notwendigen Arbeiten zur Erbringung dieser Dienstleistungen. Dies umfasst Tätigkeiten, die in den Angeboten / Leistungsbeschreibung und der AGB [https://asello.eu/agb/] konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortung des für die Verarbeitung Verantwortlichen« im Sinne des Art. 24 DSGVO).

1.2 Die Art der personenbezogenen Daten, der Verarbeitungszweck und die betroffenen Personen werden in Anlage 1 näher beschrieben.

§ 2 Dauer der Vereinbarung

2.1 Die Laufzeit der Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages betreffend der von asello bezogenen Softwaredienstleistung.

2.2 In E-Mails und Supportanfragen des Auftraggebers übermittelte Daten werden als Teil der Supportdokumentation des Auftragnehmers dauerhaft aufbewahrt. Der Auftraggeber sorgt dafür personenbezogene Daten seiner Kunden in E-Mails und Supportanfragen unkenntlich zu machen und seine Mitarbeiter entsprechend anzuweisen.

§ 3 Pflichten des Auftragnehmers

3.1 Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse (Anlage 1) ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er – sofern gesetzlich zulässig – den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

3.2 Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

3.3 Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage 2 zu entnehmen).

3.4 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation). Kosten für über den vertraglich vereinbarten Leistungsumfang hinausgehende Einzelanweisungen des Auftraggebers, sind nach Rücksprache mit dem Auftragnehmer, unter Berücksichtig des Aufwandes, vom Auftraggeber zu tragen.

3.5 Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

3.6 Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten im Auftrag des Auftraggebers zu vernichten.

3.7 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

§ 4 Pflichten des Auftraggebers

4.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4.2 Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

4.3 Die Daten werden nach dem Ende des jeweiligen Vertrages mit Ausnahme der Supportdokumentation gelöscht. Es obliegt dem Auftraggeber, Sicherungskopien von seinen Daten anzufertigen und die Daten vor Vertragsende umzuziehen. Der Auftraggeber hat selbst Zugriff auf seine Daten. Eine Pflicht des Auftragnehmers zur Herausgabe besteht daher nicht.

4.4 Der Auftraggeber verpflichtet sich dem Auftragnehmer im Rahmen von Supportanfragen keine personenbezogenen Daten Dritter zu übermitteln. Auf Verlangen des Auftraggebers löscht der Auftragnehmer die den Auftragnehmer betreffende Supportdokumentation, vorausgesetzt, der Auftraggeber entlässt ihn aus der Haftung für eigene Schäden und verpflichtet sich schriftlich den Auftragnehmer in jeder Hinsicht schad- und klaglos zu halten.

4.5 Dem Auftraggeber obliegen die aus Artikel 33, 34 DSGVO resultierenden Informationspflichten.

§ 5 Anfragen Betroffener

5.1 Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Verarbeitung von Daten dieser Person zu erteilen, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen. Dies setzt voraus, dass der Auftraggeber den Auftragnehmer hierzu schriftlich oder in Textform aufgefordert hat und der Auftraggeber dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten erstattet. Der Auftragnehmer wird keine Auskunftsverlangen beantworten und den Betroffenen insoweit an den Auftraggeber verweisen.

5.2 Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen.

§ 6 Kontrollpflichten

6.1 Der Auftraggeber kann sich auf seine Kosten vor der Aufnahme der Datenverarbeitung und sodann regelmäßig über die technischen und organisatorischen Maßnahmen des Auftragnehmers informieren und das Ergebnis dokumentieren. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich ein ggf. vorhandenes Testat eines Sachverständigen vorlegen lassen oder nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Bei der Prüfung muss mindestens ein Mitarbeiter des Auftragnehmers anwesend sein. Jeder Schritt ist mit diesem abzuklären. Entstandene Kosten für Anfahrt und Arbeitszeit des Auftragnehmers, trägt der Auftraggeber. Für die Unterstützung bei der Durchführung einer Prüfung darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Prüfung ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

6.2 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle erforderlich sind. Dafür entstehende Kosten trägt der Auftraggeber.

§ 7 Ort der Durchführung der Datenverarbeitung

7.1 Datenverarbeitungstätigkeiten werden zumindest zum Teil auch außerhalb der EU bzw. des EWR durchgeführt, und zwar in den USA.

7.2 Das angemessene Datenschutzniveau bei Verarbeitung in einem Drittland ergibt sich aus Standardvertragsklauseln, gem. Art 46 Abs 2 lit c und d DSGVO, die mit den in Anlage 3 genannten Subauftragsverarbeiter geschlossen wurden, wenn diese ihren Sitz nicht im EU/EWR-Raum haben.

§ 8 Sub- Auftragsverarbeiter

8.1 Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungspflichten verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung her-anzieht bzw. dritte Unternehmen mit Leistungen unterbeauftragt.

8.2 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten im Sinne des Art 28 Abs 4 DSGVO und aus diesem Vertrag dem Subunternehmer zu übertragen.

8.3 Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen oder Wartung.

8.4 Der Auftragnehmer wird mit diesem Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

§ 9 Informationspflichten, Schriftformklausel, Annahmeerklärung, AGB

9.1 Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

9.2 Es gilt ausschließlich österreichisches Recht.

9.3 Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

9.4 Im Übrigen gelten die Allgemeinen Geschäftsbedingungen (kurz AGB) des Auftragnehmers.

_____
Datum, Ort

_____
Auftragnehmer, Bernhard Schille

_____
Auftraggeber, firmenmäßige Zeichnung

Anlage 1 – Auflistung der personenbezogenen Daten und Zweck der Verarbeitung

1. Umfang, Art und Zweck der Datenverarbeitung

Datenverarbeitungszweck ist die Erbringung der technischen Leistungen für die Bereitstellung der Dienstleistungen der asello GmbH, wie sie in den Angeboten / Leistungsbeschreibungen und den Allgemeinen Geschäftsbedingungen (kurz AGB) der asello GmbH beschrieben werden.

Daten und Betroffene, die der Auftraggeber oder von ihm autorisierte Nutzer in der bereit gestellten Software speichern (Rechnungen, Kontakte, etc.).

2. Kunden

Art der Daten: Kundendaten, Kontaktdaten, Rechnungsdaten, Bankverbindungsdaten, Bestelldaten, Lieferdaten

Betroffene Personen: Kunden sowie Interessenten und deren Ansprechpartner

Zweck: Zur Vertragserfüllung bzw. zur Durchführung vorvertraglicher Maßnahmen

3. Mitarbeiter

Art der Daten: Mitarbeiterdaten

Betroffene Personen: Mitarbeiter

Zweck: Zur Zugangskontrolle, für Berechtigungen und Nachvollziehbarkeit von Datenänderungen

4. Lieferanten

Art der Daten: Lieferantendaten

Betroffene Personen: Lieferanten und deren Ansprechpartner

Zweck: Zur Vertragserfüllung bzw. zur Durchführung vorvertraglicher Maßnahmen

5. Mahnungen

Art der Daten: Mahnungsdaten

Betroffene Personen: Kunden sowie Interessenten und deren Ansprechpartner

Zweck: Zur Vertragserfüllung und Einbringung von geschuldeten Leistungen

○ Weitere Daten (bitte durch Komma getrennt anführen):

Art der Daten: _____

Betroffene Personen: _____

Zweck: _____

Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers

1. Vertraulichkeit

Zutrittskontrolle	ISO/IEC 27001 Zertifizierter Auftragsverarbeiter für Rechenzentrum, Versperrte Schranksysteme
Zugangskontrolle	Authentifikation mit Benutzername / Passwort, Einsatz von Anti-Viren-Software, Einsatz von Firewall, Einsatz von Intrustion-Detection-Systemen, ISO 27-0001 Zertifizierter Auftragsverarbeiter für Rechenzentrum, Zuordnung von Benutzerprofilen zu IT-Systemen, Zuordnung von Benutzerrechten
Zugriffskontrolle	Anzahl der Administratoren auf das „Notwendigste" reduziert, Anwendung eines Berechtigungskonzepts, Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
Pseudonymisierung	Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.

2. Datenintegrität

Weitergabekontrolle	Beim physischen Transport: sichere Transportbehälter/-verpackungen, Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen, Verschlüsselte Datenübertragung (TLS – Transport Layer Security)
Eingabekontrolle	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind, Berechtigungskonzept für das Lesen und Schreiben von Datenkategorien, Protokollierung von Dateneingaben, Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
Trennungsgebot	Erstellung eines Berechtigungskonzepts, Logische Mandantentrennung (softwareseitig),Trennung von Produktiv- und Testsystem

3. Verfügbarkeit und Belastbarkeit

Weitergabekontrolle	ISO 27-0001 Zertifizierter Auftragsverarbeiter für Rechenzentrum
Wiederherstellbarkeit	Erstellen eines Backup- & Recoverykonzepts, Erstellen eines Notfallplans, Testen von Datenwiederherstellung
Löschfristen	Löschkonzept für Daten, Löschkonzept für Logdateien und Metadaten

4. Evaluierungsmaßnahmen

Datenschutz Management	Regelmäßige Mitarbeiter-Datenschutz-Schulungen, Evaluierung der Datenschutzmaßnahmen (technisch- und organisatorische Maßnahmen)
Incident-Reponse-Management	Konzept für die Reaktion auf Datenschutz Verstößen
Datenschutzfreundliche Voreinstellungen	Anzahl der Administratoren auf das „Notwendigste" reduziert, Anwendung eines Berechtigungskonzepts, Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
Auftragskontrolle	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit), ISO 27-0001 Zertifizierter Auftragsverarbeiter für Rechenzentrum, schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag), Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

Anlage 3: Subauftragsverarbeiter

#	Name	Zweck	Daten	Kategorie	Drittland
1	asello Deutschland GmbH Ben-Gurion-Ring 21 60437 Frankfurt am Main Deutschland	Support	Zugriff auf alle Informationen	personenbezogen	nein
2	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	Betrieb der Serverinfrastruktur, Speicherung der Daten in einem Hochsicherheitsrechenzentrum (Niederlande, Irland - georedundant), Bereitstellung von E-Mail-Diensten, Bereitstellung von Datei-Diensten	Zugriff auf alle Informationen im Bedarfsfall	personenbezogen	Ja
3	A-Trust Landstraßer Hauptstraße 1b, E02 1030 Wien, Österreich	Bereitstellung eines Hardware Signatur Modules für die Registrierkassen Signatur	Singatur-Hash	-	Nein
4	DMS DATA+MAIL Schinnerl GmbH Gewerbeparkstraße 119 8143 Dobl, Österreich	Versand von Briefen über die asello Anwendung	Empfängeradressen der Briefe	personenbezogen	Nein
5	SendGrid Inc 1801 California Street Suite 500 Boulder, CO 80202, USA	Versand von E-Mail-Nachrichten aus der asello Anwendung	Empfänger-E-Mail-Adressen	personenbezogen	Ja
6	Host Europe GmbH Hansestrasse 111 51149 Köln Deutschland	Bereitstellung von IT-Infrastruktur	Zugriff auf alle Informationen im Bedarfsfall	personenbezogen	Nein