

Auftragsdatenverarbeitung

Vereinbarung

zwischen

hitobito AG, Belpstrasse 37, 3007 Bern
handelnd durch ihre Organe

nachfolgend «**Auftraggeberin**»

und

Puzzle ITC GmbH, Belpstrasse 37, 3007 Bern
handelnd durch ihre Organe

nachfolgend «**Auftragnehmerin**»

Inhaltsverzeichnis

A.	Gegenstand und Dauer des Auftrags.....	2
1.	Gegenstand.....	2
2.	Dauer.....	3
B.	Konkretisierung des Auftragsinhalts.....	3
1.	Art und Zweck der vorgesehenen Verarbeitung von Daten.....	3
2.	Art der Daten.....	4
3.	Kategorien der betroffenen Personen.....	5
C.	Technisch-organisatorische Massnahmen.....	5
1.	Datensicherheit.....	5
2.	Anpassung der Massnahmen.....	5
D.	Berichtigung, Einschränkung und Löschung von Daten.....	6
E.	Qualitätssicherung und sonstige Pflichten.....	6
F.	Unterauftragsverhältnisse.....	6
G.	Kontrollrechte der Auftraggeberin.....	6
H.	Löschung und Rückgabe von personenbezogenen Daten.....	7
1.	Kopien.....	7
2.	Löschen.....	7
3.	Aufbewahrung.....	7
I.	Konkrete Technisch-organisatorische Massnahmen.....	7
1.	Vertraulichkeit.....	7
2.	Integrität.....	7
3.	Verfügbarkeit und Belastbarkeit.....	8
J.	Unterschriften der Parteien.....	9

A. Gegenstand und Dauer des Auftrags

1. Gegenstand

Der Gegenstand dieser Vereinbarung (nachfolgend «Auftrag») ergibt sich aus dem Rahmenvertrag «Betrieb, Support und Wartung hitobito» vom 5.12.2019, auf den hier verwiesen wird (nachfolgend «Rahmenvertrag»).

2. Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Rahmenvertrags.

B. Konkretisierung des Auftragsinhalts

1. Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch die Auftragnehmerin ist die Bereitstellung von Cloud-Dienstleistungen für die Auftraggeberin. Die zu erbringenden Dienstleistungen ergeben sich aus dem Rahmenvertrag.

Im Rahmen des Betriebs und des Supports der jeweiligen Dienstleistung kann es insbesondere zu Zugriffen auf personenbezogene Daten der in Ziff. B..3. aufgeführten Personen kommen. Solche Zugriffe von der Auftragnehmerin auf personenbezogene Daten sind dabei jedoch lediglich ein Nebeneffekt der vereinbarten Dienstleistung und gehören nicht zu den Hauptverpflichtungen der Auftragnehmerin.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschliesslich in der Schweiz statt.

2. Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- ☒ Personenstammdaten (z. B. Name, Anschrift, Geburtsdatum, Familienstand, Berufsbezeichnung, Firmenzugehörigkeit, Lebensläufe etc.);
- ☐ Elektronische Identifikationsdaten (wie IP-Adresse, Elektronische Unterschrift, Verbindungs-/Protokolldaten, Cookies);
- ☐ Sozialdaten (d.h. alle Daten, die bspw. durch Sozialleistungsträger sowie deren Verbände und Arbeitsgemeinschaften verarbeitet werden);
- ☐ Gesundheitsdaten sowie auch genetische oder biometrische Daten;
- ☐ Auftragsdaten (z.B. Produktionsdaten, Serviceauftragsdaten, Auftragsrückmeldungen);
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail, PIN, Passwort, Ports, Login);
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse);
- ☒ Kundenstammdaten und Kundenhistorie;
- ☐ Bilder (Fotografien, Filme, etc.) / Tonaufzeichnungen;
- ☐ Vertragsabrechnungs- und Zahlungsdaten (Bank, Kontoverbindung, Kreditkartendaten);
- ☐ Planungs- und Steuerungsdaten;
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen).

3. Kategorien der betroffenen Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen ergeben sich aus der nachfolgenden Aufzählung:

- ☐ Beschäftigte;
- ☒ Kunden;
- ☐ Interessenten;
- ☒ Abonnenten;
- ☐ Lieferanten;
- ☐ Handelsvertreter;
- ☐ Ansprechpartner.

Die Kategorien enthalten jeweils ehemalige, aktuelle und potentiell künftige betroffene Personen.

C. Technisch-organisatorische Massnahmen

1. Datensicherheit

Die Auftragnehmerin hat die Datensicherheit durch geeignete Massnahmen herzustellen. Die einzelnen Massnahmen ergeben sich aus der Ziff. I. hiernach.

Es handelt sich dabei um Massnahmen der Datensicherheit und zur Gewährleistung eines angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei werden der Stand der Technik, die Kosten und die Art, der Umfang und die Zwecke der Verarbeitung berücksichtigt.

2. Anpassung der Massnahmen

Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es Auftragnehmerin gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden. Wesentliche Änderungen werden dokumentiert.

D. Berichtigung, Einschränkung und Löschung von Daten

Die Auftragnehmerin darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung der Auftraggeberin berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an die Auftragnehmerin wendet, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

E. Qualitätssicherung und sonstige Pflichten

Die Auftragnehmerin hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten; insofern gewährleistet die Auftragnehmerin insbesondere die Einhaltung folgender Vorgaben:

- Die Wahrung der Vertraulichkeit. Die Auftragnehmerin setzt bei der Durchführung der Arbeiten nur Personen oder Unterauftragnehmer ein, die zur Geheimhaltung verpflichtet und mit den relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden;
- Die Verarbeitung erfolgt ausschliesslich gemäss der Weisung der Auftraggeberin, es sei denn, dass die Auftragnehmerin gesetzlich zur Verarbeitung verpflichtet wird;
- Die umgehende Information an die Auftraggeberin über Kontrollhandlungen und Massnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen;
- Die Auftragnehmerin kontrolliert regelmässig die internen Prozesse sowie die technischen und organisatorischen Massnahmen, um zu gewährleisten, dass die Verarbeitung in ihrem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt;

F. Unterauftragsverhältnisse

Eine Auslagerung durch die Auftragnehmerin auf einen weiteren Unterauftragnehmer oder in ein Land ausserhalb der Schweiz bedarf der ausdrücklichen vorgängigen schriftlichen Zustimmung der Auftraggeberin und der Auftragnehmerin. Bei einem Wechsel des Unterauftragnehmers holt die Auftragnehmerin vorgängig die Zustimmung der Auftraggeberin ein.

G. Kontrollrechte der Auftraggeberin

Die Auftraggeberin hat das Recht, im Benehmen mit der Auftragnehmerin Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Sie hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch die Auftragnehmerin in deren Geschäftsbetrieb zu überzeugen.

H. Löschung und Rückgabe von personenbezogenen Daten

1. Kopien

Kopien oder Duplikate der Daten werden ohne Wissen der Auftraggeberin nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemässen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

2. Löschen

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch die Auftraggeberin – spätestens mit Beendigung des Dienstleistungsvertrags – hat die Auftragnehmerin sämtliche in ihrem Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, der Auftraggeberin auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

3. Aufbewahrung

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemässen Datenverarbeitung dienen, sind durch die Auftragnehmerin entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Die Auftragnehmerin kann sie zu ihrer Entlastung bei Vertragsende der Auftraggeberin übergeben.

I. Konkrete Technisch-organisatorische Massnahmen

1. Vertraulichkeit

- Zutrittskontrolle:Kein unbefugter Zutritt zu Datenverarbeitungsanlagen;
- Zugangskontrolle:Keine unbefugte Systembenutzung;
- Zugriffskontrolle:Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems;

2. Integrität

- Weitergabekontrolle:Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport;
- Eingabekontrolle:Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

3. Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle:Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust;
- Rasche Wiederherstellbarkeit.

4. Unterschriften der Parteien

Diese Vereinbarung wird jeweils in zwei Exemplaren ausgefertigt, jede Vertragspartei erhält ein beidseitig unterzeichnetes Exemplar.

hitobito AG:

Ort, Datum:

Name:

Name:

Unterschrift

Unterschrift

Puzzle ITC GmbH:

Ort, Datum:

Name:

Name:

Unterschrift

Unterschrift