Vereinbarung über die **Auftragsdatenbearbeitung**

Innov8ivelT Solutions GmbH
Schaanerstrasse 27
9490 Vaduz

Inhaltsverzeichnis

1 Einleitung

Die vorliegende Vereinbarung konkretisiert die Verpflichtungen der Parteien in Bezug auf die Vorgaben aus dem Schweizer Datenschutzgesetz (DSG) und der Datenschutzgrundverordnung der EU (EU-DSGVO). Sie ergänzt diesbezüglich die vertraglichen Vereinbarungen ("Vertrag") zwischen IITS und dem Kunden. Es kann sich dabei um einen einzelnen oder mehrere Verträge zwischen IITS und dem Kunden handeln, in welcher IITS als Leistungserbringerin gegenüber dem Kunden auftritt.

Die vorliegende Vereinbarung gilt nur insofern und insoweit als die nachfolgenden Voraussetzungen erfüllt sind:

1. Der Kunde ist entweder Verantwortlicher oder Auftragsbearbeiter im Anwendungsbereich des DSG und/oder der EU-DSGVO und

2. der Kunde zieht IITS im Rahmen des Vertrages als Auftragsbearbeiter oder Unter-Auftragsbearbeiter für die Bearbeitung von Personendaten bzw. von personenbezogenen Daten bei, welche vom Anwendungsbereich des DSG und/oder der EU-DSGVO erfasst sind ("relevante Daten").

2 Gegenstand, Dauer und Art der Datenbearbeitung

Gegenstand, Dauer sowie Art und Zweck der Bearbeitung ergeben sich aus dem Vertrag. Die Kategorien der bearbeiteten relevanten Daten, die Kategorien betroffener Personen sowie die zu treffenden technischen und organisatorischen Massnahmen („TOM“) sind im Anhang dieser Vereinbarung aufgeführt.

3 Anwendungsbereich und Verantwortlichkeit

IITS bearbeitet die relevanten Daten ausschliesslich zum Zweck der Vertragserfüllung bzw. zu den im Vertrag genannten Zwecken. Der Kunde ist für die Rechtmäßigkeit der Datenbearbeitung an sich, inklusive der Zulässigkeit der Auftrags-/Unter-Auftragsbearbeitung, verantwortlich.

Die Weisungen des Kunden sind in dieser Vereinbarung und dem Vertrag dokumentiert. Der Kunde hat das Recht, IITS jederzeit schriftlich darüberhinausgehende Weisungen in Bezug auf die Bearbeitung der relevanten Daten zu erteilen. IITS kommt diesen Weisungen nach, soweit diese im Rahmen der vertraglich vereinbarten Leistungen durch IITS umsetzbar und objektiv zumutbar sind. Führen solche Weisungen zu Mehrkosten von IITS oder einem geänderten Leistungsumfang, so ist das vertraglich vereinbarte Vertragsänderungsverfahren anwendbar.

IITS informiert den Kunden unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen das DSG oder die EU-DSGVO verstößt. IITS darf diesfalls die Umsetzung der Weisung so lange aussetzen, bis sie vom Kunden bestätigt oder abgeändert wurde. Bei Weisungen des Kunden im Zusammenhang mit der Vergabe von Zugriffsberechtigungen oder der Herausgabe von relevanten Daten an den Kunden selbst gilt das Vorstehende nicht, und IITS darf jederzeit davon ausgehen, dass diese Weisungen gesetzeskonform sind. Sie ist jedoch berechtigt, vom Kunden entsprechende schriftliche Bestätigungen zu verlangen.

4 Pflichten von IITS

IITS bearbeitet die relevanten Daten ausschliesslich gemäss den Bestimmungen aus dem Vertrag und dieser Vereinbarung. Vorbehalten bleibt die Erfüllung gesetzlicher, regulatorischer oder behördlicher Verpflichtungen durch IITS.

IITS wird die im Vertrag und den Anhängen zu dieser Vereinbarung definierten TOM zum Schutz der relevanten Daten treffen. IITS darf die vereinbarten TOM jederzeit anpassen, solange das vereinbarte Schutzniveau nicht unterschritten wird. Zudem überprüft IITS laufend die vereinbarten TOM auf den aktuellen Stand der Technik und schlägt dem Kunden gegebenenfalls die Implementierung zusätzlicher Massnahmen vor, welche im Rahmen eines Vertragsnachtrags vereinbart werden können.

IITS verpflichtet sich, in Bezug auf die relevanten Daten ein Verzeichnis von Bearbeitungstätigkeiten im Einklang mit Art. 12 Abs. 1 DSG bzw. Art. 30 Abs. 2 EU-DSGVO zu führen. IITS wird dem Kunden jederzeit auf Anfrage Einblick in die Teile dieses Verzeichnis gewähren, die von der Leistungserbringung von IITS ihm gegenüber betroffen sind.

IITS stellt sicher, dass es den mit der Bearbeitung der relevanten Daten des Kunden befassten Mitarbeitenden und anderen Hilfspersonen von IITS untersagt ist, die relevanten Daten zu anderen als den im Vertrag genannten Zwecken und abweichend von dieser Vereinbarung zu bearbeiten. Ferner stellt IITS sicher, dass sich die zur Bearbeitung der relevanten Daten befugten Personen zur Vertraulichkeit verpflichtet haben und/oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Vertrages fort.

IITS unterrichtet den Kunden unverzüglich, wenn ihr Verletzungen des Schutzes der relevanten Daten bei IITS oder einem ihrer Unter-Auftragsbearbeiter bekannt werden (Data Breach). IITS informiert den Kunden schriftlich (E-Mail ausreichend) in angemessener Weise über Art und Ausmaß der Verletzung sowie mögliche Abhilfemassnahmen. Die Parteien treffen in so einem Fall die erforderlichen Massnahmen zur Sicherstellung des Schutzes der relevanten Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen sowie die Parteien und sprechen sich hierzu unverzüglich ab.

IITS nennt dem Kunden den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen sowie in den Fällen, in denen dies gemäss Art. 37 EU-DSGVO vorgeschrieben ist, den Datenschutzbeauftragten.

IITS verpflichtet sich, den Kunden auf Wunsch und gegen vorgängig vereinbarte separate Vergütung im Rahmen ihrer Möglichkeiten bei der Erfüllung der Rechte der betroffenen Personen gegenüber dem Kunden gemäss Kapitel 4 des DSG bzw. Kapitel III der EU-DSGVO zu unterstützen. Darüber hinaus kann IITS dem Kunden gegen separate Vergütung weitergehende Unterstützung des Kunden, z.B. im Zusammenhang mit einer Datenschutzfolgeabschätzung, Konsultation der Aufsichtsbehörde, Meldungen an diese etc. anbieten.

Relevante Daten sind nach Vertragsende gemäss den vertraglichen Bestimmungen herauszugeben oder zu löschen. IITS setzt für die Löschung von relevanten Daten in der IT-Branche etablierte Verfahren ein.

5 Pflichten und Obliegenheiten des Kunden

Der Kunde trifft in seinem Verantwortungsbereich (z.B. auf seinen eigenen Systemen, Gebäuden, Applikationen/Umgebungen in seiner Betriebsverantwortung) selbständig angemessene technische und organisatorische Massnahmen zum Schutz der relevanten Daten.

Der Kunde hat IITS unverzüglich zu informieren, wenn er in der Leistungserbringung von IITS Verletzungen datenschutzrechtlicher Bestimmungen feststellt.

Der Kunde nennt IITS den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen sowie in den Fällen, in denen dies gemäss Art. 37 EU-DSGVO vorgeschrieben ist, den Datenschutzbeauftragten.

6 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung, Auskunft oder anderen Ansprüchen zu relevanten Daten direkt an IITS, wird IITS die betroffene Person an den Kunden verweisen, sofern eine Zuordnung an den Kunden nach Angaben der betroffenen Person möglich ist. Die Unterstützung des Kunden seitens IITS bei Anfragen betroffener Personen richtet sich nach Ziffer 4.

7 Nachweismöglichkeiten, Berichte und Audits

IITS ist verpflichtet, dem Kunden auf Verlangen Informationen zur Verfügung zu stellen, um die Einhaltung der Pflichten gemäss dieser Vereinbarung zu dokumentieren.

Die Parteien halten fest, dass die Einhaltung dieser Verpflichtung grundsätzlich dadurch belegt wird, dass IITS nach ISO 27001 zertifiziert ist oder IITS dem Kunden zu bestimmten Bereichen Berichte oder ähnliche durch einen unabhängigen Dritten erstellte Auditberichte oder Bestätigungen über im Vertrag speziell erwähnte Zertifizierungen etc. zur Verfügung stellt. Im Vertrag allfällig definierte Audit-Rechte sowie gesetzlich zwingend vorgeschriebene Prüfrechte des Kunden oder seiner Aufsichtsbehörden bleiben vorbehalten. Auf jeden Fall sind im Rahmen solcher Audits der Grundsatz der Verhältnismäßigkeit einzuhalten sowie die schutzwürdigen Interessen von IITS (namentlich an Geheimhaltung) angemessen zu berücksichtigen. Vorbehältlich einer abweichenden Regelung trägt der Kunde sämtliche Kosten solcher Audits (inklusive nachgewiesene interne Kosten von IITS, die bei der Mitwirkung am Audit entstehen).

Werden nach Vorlage von Nachweisen oder Berichten oder im Rahmen eines Audits Verletzungen dieser Vereinbarung oder Mängel bei der Umsetzung der Pflichten von IITS festgestellt, so hat IITS unverzüglich und kostenlos geeignete Korrekturmassnahmen zu implementieren.

8 Beizug von Unter-Auftragsbearbeitern

Soweit der Vertrag keine einschränken deren Bestimmungen zum Beizug Dritter enthält, ist IITS zum Beizug von Unter-Auftragsbearbeitern berechtigt, hat jedoch den Kunden vorgängig darüber zu informieren, wenn sie nach Inkrafttreten dieser Vereinbarung neue Unter-Auftragsbearbeiter beizieht oder bestehende Unter-Auftragsbearbeiter austauscht. Der Kunde kann gegen den Beizug eines neuen oder den Austausch eines bestehenden Unter-Auftragsbearbeiters aus wichtigen datenschutzrechtlichen Gründen schriftlich innerhalb einer Frist von 30 Tagen Einspruch erheben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Kunden ein Kündigungsrecht in Bezug auf die hiervon betroffene Leistung eingeräumt. IITS wird mit ihren Unter-Auftragsbearbeitern im erforderlichen Umfang Vereinbarungen treffen, um die Verpflichtungen gemäss vorliegender Vereinbarung sicherzustellen.

9 Bekanntgabe ins Ausland

Jedwede Bekanntgabe von relevanten Daten durch IITS ins Ausland oder an eine internationale Organisation ist nur zulässig, wenn IITS die Bestimmungen von Art. 16 ff. DSG bzw. von Kapitel V EUDSGVO einhält. Soweit hingegen eine solche Bekanntgabe von relevanten Daten vom Kunden gewünscht bzw. in seinem Auftrag erfolgt, obliegt die Einhaltung der entsprechenden Bestimmungen ausschliesslich dem Kunden.

10 Schlussbestimmungen

Die Artikelnummern des DSG beziehen sich auf das revidierte DSG (BBl 2020 7639). Vor dessen Inkrafttreten gelten die vorliegend vereinbarten Bestimmungen sinngemäß. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit aller Verträge zwischen IITS und dem Kunden, unter welchen IITS für den Kunden relevante Daten bearbeitet, sofern sich aus den Bestimmungen dieser Vereinbarung nicht länger dauernde Verpflichtungen ergeben.

In Abweichung allfälliger Schriftformvorbehalte im Vertrag kann die vorliegende Vereinbarung auch auf elektronischem Weg zwischen den Parteien vereinbart oder geändert werden.

Die Pflichten aus dieser Vereinbarung gelten zusätzlich zu den im Vertrag festgelegten Pflichten und schränken letztere nicht ein. In Bezug auf die in einem Anhang zu dieser Vereinbarung generisch festgelegten TOM gehen im Widerspruchsfall die Regelungen des Vertrages vor. Im Übrigen gelten die Regelungen des Vertrages unverändert weiter.

Anhang

1 Verwendete Datenelemente

1.1 Generell

Der Kunde überlasst IITS im Rahmen der Verträge in seinem eigenen Ermessen und in seinem Auftrag Personendaten zur Bearbeitung.

1.2 Betroffene Personen

Es kann sich dabei um Personendaten insbesondere folgender betroffener Personen handeln:

- Potenzielle Kunden, Kunden, Geschäftspartner, Verkäufer und Händler des Kunden – welche natürlichen Personen sind
- Mitarbeitende oder andere Hilfspersonen von potenziellen Kunden, Kunden, Geschäftspartnern, Verkäufern, oder Händlern
- Mitarbeitende oder andere Hilfspersonen des Kunden, welche durch den Kunden berechtig wurden die Services zu nutzen

1.3 Art von Personendaten

Es kann sich dabei insbesondere um folgende Arten von Personendaten handeln:

- Persönliche Informationen wie Vorname, Name, Geburtsdatum, Alter, Geschlecht, Nationalität etc.
- Geschäftliche Kontaktdaten wie E-Mailadresse, Telefonnummer, Adresse
- Private Kontaktdaten wie E-Mailadresse, Telefonnummer, Adresse
- Informationen über das Berufsleben wie Stellenbezeichnung, Funktion etc.
- Benutzerinformationen wie Logindaten, Kundennummer, Personalnummer etc.
- Technische Informationen wie IP-Adresse, Geräteinformationen etc.

1.4 Besonders schützenswerte Personendaten

Bei diesen Datenkategorien handelt es sich um Personendaten aus denen die rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

1.5 Geheimnisgebundene Daten

Bei diesen Daten kann es sich beispielsweise um dem Berufsgeheimnis, dem Bankgeheimnis, dem Amtsgeheimnis, der Verschwiegenheitspflicht gemäss Sozialversicherungsrecht unterliegende Daten handeln.

2 Technische und organisatorische Massnahmen

Die folgenden Kapitel beschreiben die von der IITS getroffenen Massnahmen in Bezug auf den Schutz von Personendaten im Rahmen der Auftragsdatenbearbeitung. Die nachstehend aufgeführten Massnahmen sind

generisch zu verstehen und kommen jeweils dann zur Anwendung, wenn im Vertrag nichts Abweichendes definiert ist.

2.1 Zugriffskontrolle (Daten)

IITS hat (unter anderem) die folgenden Massnahmen ergriffen, um sicherzustellen, dass Nutzer nur auf diejenigen Daten Zugriff haben, für die sie autorisiert sind und um zu vermeiden, dass personenbezogene Daten ohne Autorisierung gelesen werden können:

- Einsatz rollenbasierten Autorisierungskonzept nach Need-to-Know Prinzip
- Anzahl Administratoren auf nötiges Minimum reduziert
- Protokollierung von Applikationszugriffen
- Sichere Medienbereinigung vor der Wiederverwendung
- Verwendung von Schreddern
- Verschlüsselung transportierter Daten mit TLS
- Rechteverwaltung durch Systemadministratoren
- Passwort-Richtlinie mit geltenden Mindestanforderungen an Passwortkomplexität
- Konforme Zerstörung von Datenträgern
- Kontrolle der Berechtigungen bei Eintritt und Austritt von Mitarbeitenden

2.2 Übertragungskontrolle

IITS hat (unter anderem) die folgenden Massnahmen ergriffen, um sicherzustellen, dass personenbezogene Daten nicht gelesen, kopiert, oder modifiziert werden können während der elektronischen Übermittlung, des Transports oder der Speicherung:

- Einsatz einer Standleitung und/oder VPN-Verbindungen
- Verschlüsselung transportierter Daten mit TLS
- Dokumentation der Datenempfänger und der Übertragungszeiten
- Für den physischen Transport, sorgfältige Auswahl des Transportpersonals und der Fahrzeuge und sowie Verschlüsselung des genutzten Speichermediums
- Datenoffenbarung nur in anonymisierter oder pseudonymisierter Form

2.3 Eingabekontrolle

IITS hat (unter anderem) die folgenden Massnahmen ergriffen, um sicherzustellen, dass es möglich ist nachzuvollziehen und zu kontrollieren, ob und wer personenbezogene Daten eingibt, modifiziert oder aus Datenverarbeitungssystem löscht:

- Protokollierung der Eingabe, Modifikation und Löschung von Daten
- Rückverfolgbarkeit der Eingabe, Modifikation und Löschung von Daten durch individuelle Benutzerprofile
- Rechtevergabe für Eingabe, Modifikation und Löschung von Daten basierend auf einem Autorisierungskonzept

2.4 Auftragskontrolle

IITS hat (unter anderem) die folgenden Massnahmen ergriffen, um sicherzustellen, dass in seinem Auftrag und im Einvernehmen mit dem Verantwortlichen weiterverarbeitete Date nur auf dessen Weisung hin verarbeitet werden:

- Sorgfältige Auswahl der Unterauftragnehmer unter Berücksichtigung ihrer Historie (insbesondere hinsichtlich Informationssicherheit)
- Schriftliche Weisungen an Unterauftragnehmer (über Vereinbarung der Auftragsdatenverarbeitung)
- Sicherstellen, dass Unterauftragnehmer Datenschutzbeauftragten ernannt haben
- Effektive Kontrollrechte zugesichert durch Auftragsverarbeiter
- Vorgängige Prüfung der Dokumentation und der Sicherheitsmaßnahmen, die Unterauftragnehmer ergriffen haben
- Verpflichtung der Mitarbeitenden des Auftragsverarbeiters zur Wahrung der Vertraulichkeit
- Sichere Löschung der Daten nach Vertragsende
- Fortlaufende Überwachung der Unterauftragnehmer und deren Aktivitäten

2.5 Trennungskontrolle

IITS hat (unter anderem) die folgenden Massnahmen ergriffen, um sicherzustellen, dass Daten, die zu verschiedenen Zwecken erhoben wurden, separat verarbeitet werden können:

- Sicherstellung, dass Daten der Kunden nicht gegenseitig einsehbar sind durch logische oder physische Trennung
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und Speicherung auf einem separat gesicherten IT-System
- Trennung von Produktiv- und Testsystemen