Auftragsbearbeitungsvertrag

Dieser Auftragsbearbeitungsvertrag konkretisiert die Verpflichtungen betreffend Datenschutz, welche sich aus dem Vertragsverhältnis zwischen der agiflex GmbH (nachfolgend "Provider" oder "Auftragsbearbeiter") und ihren Kundinnen und Kunden (nachfolgend "Auftraggeber" oder "Verantwortlicher") ergeben. Für sämtliche anfallende Datenschutzfragen kann der Auftraggeber den Datenschutzbeauftragen des Providers über info@agiflex.ch erreichen.

Präambel
Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem zwischen den Parteien geschlossenen Vertrag ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Providers oder durch den Provider Beauftragte personenbezogene Daten (nachfolgend „Daten“) des Auftraggebers verarbeiten.

1. **Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung**
   a. Zwischen den Parteien besteht ein Rechtsverhältnis, für dessen Durchführung Personendaten vom Verantwortlichen an den Auftragsbearbeiter übertragen werden ("Hauptvertrag"). Grundlage für das Rechtsverhältnis der Parteien bilden die Allgemeinen Geschäftsbedingungen ("AGB") des Providers. Der vorliegende Auftragsbearbeitungsvertrag wird zwischen den Parteien geschlossen, um bei der Übertragung von Personendaten einen angemessenen Schutz zu gewährleisten.
   b. Solange in dieser Vereinbarung nicht abweichend bestimmt, sollen alle Begrifflichkeiten dieselbe Bedeutung haben, wie im Schweizer Datenschutzgesetz ("DSG"). Ferner unterstützt diese Vereinbarung die Parteien bei der Einhaltung der Datenschutz-Grundverordnung der EU ("DSGVO"), soweit diesbezüglich geschützte Personendaten von Kunden aus dem EU-Raum betroffen sind.
   c. Einzelheiten in Bezug auf die Dienstleistung des Providers sind in dem jeweiligen Vertrag zwischen Provider und Auftraggeber (nachfolgend „Vertrag“) geregelt.
   d. Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung, sofern im Vertrag nichts Abweichendes aufgeführt ist.
   e. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages.

2. **Beschreibung der Datenbearbeitung**
   a. Der Provider bearbeitet Personendaten im Auftrag des Auftraggebers. Gegenstand und Dauer des Vertragsverhältnisses sowie Art und Zweck der Bearbeitungen ergeben sich grundsätzlich aus den AGB sowie dem Anhang A und B zum Auftragsbearbeitungsvertrag.
   b. Durch Ausfüllen der Anmeldemaske zur Registrierung und Bestellung eines Benutzerkontos auf der Website des Providers erteilt der Auftraggeber dem Provider die entsprechende Weisung zur Datenbearbeitung. Der Auftraggeber kann seine Weisungen in seinem Konto oder durch Mitteilung an den Provider ergänzen, ändern oder zurückziehen. Weisungen, die in den AGB nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich durch den Auftraggeber nachzuholen. Der Provider verarbeitet die im Vertrag genannten Daten im Auftrag des Auftraggebers zu dem dort genannten Zweck in dem genannten Umfang. Dies umfasst Tätigkeiten, die im Vertrag konkretisiert sind.

3. **Pflichten des Providers**
   a. Der Provider darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten; ausser es liegt ein gesetzlich geregelter Ausnahmefall vor. Der Provider informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstösst. Der Provider darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
   b. Der Provider wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Massnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den jeweiligen gesetzlichen Anforderungen genügen. Der Provider hat technische und

organisatorische Massnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Massnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

c. Der Provider gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so aus, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft technische und organisatorische Massnahmen zum angemessenen Schutz der Personendaten des Auftraggebers, die den jeweiligen gesetzlichen Anforderungen genügen. Der Auftragsbearbeiter hat dabei den Stand der Technik, die Implementierungskosten und die Art, den Umfang und die Zwecke der Bearbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Grund- und Persönlichkeitsrechte betroffener Personen berücksichtigt. Die Massnahmen sind in Anhang B beschrieben und werden periodisch überprüft. Änderungen der Massnahmen sind zulässig, sofern das bisherige Sicherheitsniveau nicht unterschritten wird. Dem Auftraggeber sind diese technischen und organisatorischen Massnahmen bekannt und erträgt die Verantwortung dafür, dass diese für die Risiken der zu bearbeitenden Daten ein angemessenes Schutzniveau bieten.
d. Der Provider unterstützt so weit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen sowie bei der Einhaltung der datenschutzrechtlichen Pflichten.
e. Der Provider gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Provider tätigen Personen untersagt ist, die Daten ausserhalb der Weisung zu verarbeiten. Ferner gewährleistet der Provider, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
f. Der Provider unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Provider trifft die erforderlichen Massnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
g. Der Provider nennt dem Auftraggeber den folgenden Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen: Der Datenschutzbeauftragte der agiflex GmbH ist Roger Frick.
h. Der Provider gewährleistet, seinen jeweiligen datenschutzrechtlichen Pflichten nachzukommen und ein Verfahren zur regelmässigen Überprüfung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
i. Der Provider berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Provider die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.
j. In besonderen, vom Auftraggeber zu bestimmenden, Fällen erfolgt eine Aufbewahrung bzw. Übergabe von Datenträgern oder Daten auf Wunsch des Auftraggebers. Vergütung und Schutzmassnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.
k. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
l. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person im Zusammenhang mit der Auftragsverarbeitung, verpflichtet sich der Provider den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.
m. Leistungen wie die Herausgabe von Datenträgern, Ansprache von Betroffenen, Prüfungen sind dem Provider gemäss seiner aktuellen Stundensätze bzw. externer Aufwände zu vergüten.

4. Pflichten des Auftraggebers

a. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen

der Datenschutzgesetze, insbesondere für die Rechtmässigkeit der Datenweitergabe an den Provider sowie für die Rechtmässigkeit der Datenverarbeitung allein verantwortlich.

b. Der Auftraggeber hat sich davon überzeugt, dass die durch den Auftragsbearbeiter eingesetzten, in Anhang B beschriebenen, technischen und organisatorischen Massnahmen ("TOM") ausreichend sind, um für die übertragenen Personendaten einen angemessenen Datenschutz sicherzustellen.
c. Der Auftraggeber hat den Provider unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmässigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
d. Der Auftraggeber nennt dem Provider den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen, sofern dieser von den durch den Auftraggeber bereits benannten Ansprechpartnern abweicht.

5. Anfragen betroffener Personen

a. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Provider, wird der Provider die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Provider leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Provider unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Provider haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6. Nachweismöglichkeiten

a. Der Provider weist dem Auftraggeber die Einhaltung der in dieser Anlage niedergelegten Pflichten mit geeigneten Mitteln nach. Dies erfolgt durch einen Selbstaudit.
b. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Provider darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Massnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Provider stehen, hat der Provider gegen diesen ein Einspruchsrecht.
c. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoss nach dem Strafgesetzbuch strafbewehrt ist.

7. Subunternehmer (weitere Auftragsverarbeiter)

a. Die Beauftragung von Subunternehmern durch den Provider ist zulässig, soweit diese im Umfang des Unterauftrags ihrerseits die Anforderungen der vorliegenden Anlage erfüllen. Aktuell arbeitet der Provider nur mit Microsoft Azure Schweiz zusammen. Die Microsoft Schweiz GmbH ist die 1983 gegründete Tochtergesellschaft der Microsoft Corporation/Redmond, U.S.A., des weltweit führenden Herstellers von Standardsoftware.
b. Der Auftraggeber stimmt zu, dass der Provider Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Provider den Auftraggeber. Der Provider ist verpflichtet den Auftraggeber über die Beauftragung eines Subunternehmers durch Aktualisierung der eben genannten Übersicht zu informieren. Die Übersicht ist jeweils mindestens 14 Tage vorab zu aktualisieren. Der Auftraggeber wird regelmässig die Übersicht einsehen. Der Auftraggeber kann der Änderung – innerhalb dieser 14 Tage – aus wichtigem Grund – gegenüber dem Provider widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Provider ein Sonderkündigungsrecht eingeräumt.
c. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Provider weitere Provider mit der ganzen oder einer Teilleistung der in dieser Anlage vereinbarten Leistung beauftragt. Der

Provider wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmassnahmen zu gewährleisten. Subunternehmer, welche keinen Zugriff auf Kundendaten haben bzw. keine Bearbeitung von Kundendaten vornehmen, sind von diesem Kapitel ausgenommen und werden entsprechend nicht in der genannten Liste erscheinen.

d. Erteilt der Provider Aufträge an Subunternehmer, so obliegt es dem Provider, seine datenschutzrechtlichen Pflichten aus dieser Anlage dem Subunternehmer zu übertragen.

8. Informationspflichten

a. Sollten die Daten des Auftraggebers beim Provider durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Massnahmen Dritter gefährdet werden, so hat der Provider den Auftraggeber unverzüglich darüber zu informieren.
b. Der Provider wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschliesslich beim Auftraggeber als „Verantwortlicher“ im Sinne der Datenschutzverordnungen liegen.

9. Haftung

a. Die Haftung richtet sich nach dem Vertrag.

10. Sonstiges

a. Im Übrigen gelten die Regelungen des Vertrags. Bei etwaigen Widersprüchen zwischen Regelungen dieser Anlage und den Regelungen des Vertrages geht diese Anlage vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit des Vertrags und der Anlage im Übrigen nicht.
b. Anhang A und B ist wesentlicher Bestandteil dieses Vertrages.

Anhang A zur Auftragsverarbeitungsvereinbarung

Gegenstand des Auftrags:	Verarbeitung von personenbezogenen Daten des Auftraggebers im Rahmen seiner Nutzung der Leistungen des Providers als Software as a Service.
Art und Zweck der vorgesehenen Verarbeitung von Daten:	Die vom Auftraggeber verarbeiteten personenbezogenen Daten werden an den Provider im Rahmen der Software as a Service Leistungen übertragen. Der Provider verarbeitet diese Daten ausschliesslich nach der getroffenen Vereinbarung (Zeiterfassung, Fälle, Kommen&Gehen, Journal, Dokumentenablage).
Art der personenbezogenen Daten:	Die Datenarten hängen von den durch den Auftraggeber übermittelten Daten ab: • Falldaten (Name, Geburtsdatum einschliesslich der weiteren besonders schützenswerten Falldaten) • Historie der Falldaten
Kategorien betroffener Personen:	Die Kategorien der betroffenen Personen hängen von den durch den Auftraggeber übermittelten Daten ab: • Anwender*innen des Auftraggebers • Falldaten des Auftraggebers • Kontaktdaten zu Ansprechpartnern
Löschung, Sperrung und Berichtigung von Daten:	Anfragen zur Löschung, Sperrung und Berichtigung sind an den Auftraggeber zu richten; im Übrigen gelten die Regelungen des Vertrages.

Anhang B - Technische und organisatorische Massnahmen (TOM)

I. Zutrittskontrolle:

Massnahmen, mit denen Unbefugten der Zutritt zu Datenbearbeitungsanlagen verwehrt wird, mit denen Personendaten bearbeitet oder genutzt werden:

- Alarmsystem
- Automatisierte Zutrittskontrolle
- Schlüssel-Management (Schlüssel-Herausgabe, etc.)
- Manuelles Verschlusssystem (auf Schlüsselpersonen beschränkte Nutzung bei Fehler in Zutrittskontrollsystemen)
- Festlegung zutrittsberechtigter Personen
- Da wir mit MS Azure Germany arbeiten, hat keine unserer Personen physischen Zugriff auf die Serverinfrastruktur

II. Zugangskontrolle:

Massnahmen, mit denen die Nutzung von Datenbearbeitungssystemen durch Unbefugte verhindert wird:

- Vergabe von Benutzerrechten
- Passwortvergabe
- Authentifizierung mit Benutzername / Passwort / MFA
- Automatische Zugangssperre
- Manuelle Zugangssperre
- Protokollierung des Zugangs
- Verwendung von Hardware Firewalls
- Verwendung von User Profilen
- Zusätzliche Massnahmen: Web-Application Firewalls, regelmässige Vulnerability Scans, regelmässiges Penetration Testing, Patch Management, Minimalvoraussetzungen für Passwortkomplexität und erzwungener Passwortwechsel, Verwendung von Virenscannern.
- Zuordnung von User Profilen zu IT-Systemen
- Verwendung von VPN-Technologie
- Verwendung eines Mobile-Device-Managements (zum Beispiel: Remote Locking and Wiping von Smartphones)
- Hardwareverschlüsselung für Notebooks

III. Zugriffskontrolle:

Massnahmen, die gewährleisten, dass die zur Benutzung eines Datenbearbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass Personendaten bei der Bearbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:

- Schaffung eines Autorisierungskonzepts (Identity Access Management)
- Anzahl Administratoren aufs “absolute Minimum” reduziert
- Vergabe minimaler Berechtigungen
- Umsetzen von Zugriffsbeschränkungen
- Sichere Medienbereinigung vor der Wiederverwendung
- Hardwareverschlüsselung (Backup-Tapes, Notebooks)
- Rechteverwaltung durch Systemadministratoren
- Passwort-Richtlinie mit Vorgaben zur Passwortlänge, Passwort Change-Management
- Sichere Aufbewahrung von Datenträgern

IV. Bekanntgabekontrolle

Massnahmen, die gewährleisten, dass Personendaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung

von Personendaten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Schaffung einer Standleitung oder einer VPN-Verbindung
- Verschlüsselung (Backup für Off-site-Speicherung)
- TLS-Verschlüsselung für alle Kommunikation (Web-Client, APIs, mobile Apps)
- Sicherung der Übertragung im Backend
- Sicherung der Übertragung zu externen Systemen
- Implementation von Sicherheitsgateways an den Netzübergabepunkten
- Härtung der Backendsysteme
- Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder
- Maschine-Maschine-Authentisierung
- Datenschutzgerechtes Lösch-/ Zerstörungsverfahren

V. Eingabekontrolle

Massnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem Personendaten in Datenbearbeitungssystemen eingegeben, verändert oder entfernt werden können:

- Rechtevergabe für Eingabe, Modifikation und Löschung von Daten basierend auf einem Authorisierungskonzept
- Automatische Dokumentation der Eingabeberechtigungen
- Protokollierung der Eingaben

VI. Verfügbarkeitskontrolle

Massnahmen, die gewährleisten, dass Personendaten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Unterbrechungsfreie Stromversorgung (UPS)
- Vorrichtungen, um Temperatur und Feuchtigkeit in Serverräumen zu überwachen
- Feuer- und Rauchmeldesysteme
- Alarmierung, wenn unbefugter Zutritt zu Serverräumen erfolgt
- Schaffung von Backup- & Wiederherstellungskonzepten
- Erstellen von Datenbackups
- Testen der Datenwiederherstellung
- Sichere Off-site-Speicher von Datenbackups
- Klimaanlagen in Serverräumen
- Löschanlagen in Serverräumen

VII. Gebot der Trennung

Massnahmen, die gewährleisten, dass Personendaten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt bearbeitet werden:

- Schaffung eines Autorisierungskonzepts
- Bewilligte und dokumentierte Datenbankrechte
- Logical Client Separation/logische Mandantentrennung (auf Stufe Software)
- Trennung von produktiven und Testsystemen
- Sparsamkeit bei der Datenerhebung

Letzte Aktualisierung Januar 2025