Anlage **Auftragsverarbeitungsvertrag** (AVV) zu den Allgemeinen Geschäftsbedingungen (AGB)

0 Einführung

Der «AVV» definiert die datenschutzrechtlichen Rechte und Pflichten beider Parteien auf der Grundlage der aktuellen Datenschutzgesetzgebung, insbesondere des revidierten schweizerischen Bundesgesetzes über den Datenschutz «DSG» (1. September 2023) und der Datenschutz-Grundverordnung der Europäischen Union «DSGVO» (25. Mai 2018). Die in diesem «AVV» verwendeten Begriffe sind so zu verstehen, wie sie in der «DSG» definiert sind.

Vereinbarung

zwischen

dem Kunden

im Folgenden „Auftraggeber“ genannt

und

openconcept AG

Busswilstrasse 2

3250 Lyss

Schweiz

im Folgenden „Anbieter“ genannt

über die Auftragsverarbeitung.

1 Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem zwischen den Parteien geschlossenen Vertrag (AGB des Anbieters) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Mitarbeiter des Anbieters oder durch den Anbieter beauftragte Dritte, Personendaten (im Folgenden „Daten“ genannt) des Auftraggebers bearbeiten (Art. 5 DSG; Art. 4 DSGVO). Ausserdem wird sichergestellt, dass die Bearbeitung der Daten in Übereinstimmung mit den geltenden datenschutzrechtlichen Bestimmungen und unter Berücksichtigung der Rechte und Interessen der betroffenen Personen erfolgt.

2 Ort der Datenbearbeitung

Die Datenbearbeitung erfolgt ausschliesslich in der Schweiz. Die Applikationsserver von «timesaver» stehen in zwei mehrfach zertifizierten und gesicherten Rechenzentren in der Schweiz.

Es ist erforderlich, dass der Verantwortliche vorher die Übermittlung von Personendaten in ein Drittland oder an eine internationale Organisation genehmigt. Diese darf in jedem Fall nur dann erteilt werden, wenn die besonderen Voraussetzungen der Art. 14 bis 18 DSG und Art. 44 bis 50 DSGVO erfüllt sind.

3 Dauer und Gegenstand der Bearbeitung

Einzelheiten in Bezug auf die Leistungen des Anbieters sind in dem jeweiligen Vertrag zwischen Anbieter und Auftraggeber (im Folgenden „Vertrag“ genannt) geregelt, dieser Vertrag besteht aus den AGB des Anbieters.

Gegenstand:

Bearbeitung von Daten des Auftraggebers im Rahmen seiner Nutzung von timesaver, der Software-as-a-Service-Dienstleistung des Anbieters.

Dauer:

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages. Es ist zu beachten, dass nach Beendigung des Vertrages die Daten des Auftraggebers gemäss den geltenden gesetzlichen Bestimmungen gelöscht werden, sofern sich nicht aus den Bestimmungen dieser Anlage darüberhinausgehende Verpflichtungen ergeben.

4 Art und Zweck der Bearbeitung

Die vom Auftraggeber verarbeiteten Daten werden im Rahmen der Nutzung von Timesaver, der Software-as-a-Service-Dienstleistung, an den Anbieter übertragen. Die Bearbeitung dieser Daten umfasst (Art. 5 DSG; Art. 4 DSVGO): das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreiten oder einer anderen Form der Bereitstellung, Abgleichen oder Verknüpfen, Einschränken, Löschen oder Vernichten der Daten.

Art der personenbezogenen Daten:

Die Datenarten hängen von den durch den Auftraggeber übermittelten Daten ab. Diese sind (abhängig vom Auftrag):

- Personenstammdaten (Name, Vorname, Personalcode/-nummer, NFC-ID, API-Key)
- Kontaktdaten (E-Mailadresse)
- Onlinekennungen (Cookie-Kennung, IP-Adresse)
- Besonders schützenswerte Daten (Abwesenheitsdaten «Arbeitsunfähig/Krank»)
- Vertragsdaten vom Auftraggeber einschliesslich Kontaktdaten (Name, postalisch Anschrift, E-Mailadresse)
- Kundendaten von Kunden des Auftraggebers (Kundenname) einschliesslich Kontaktdaten (E-Mailadresse)

Kategorien der betroffenen Personen:

Die Kategorien der betroffenen Personen hängen von den durch den Auftraggeber genutzten Funktionen und den dazu übermittelten Daten ab. Diese sind (abhängig vom Auftrag):

- Mitarbeiter des Auftraggebers
- Auftraggeber
- Kunden des Auftraggebers

Zweck:

Der Anbieter verarbeitet diese Daten ausschliesslich nach zum Zweck der getroffenen Vereinbarung. Dieser ist (abhängig vom Auftrag):

- Arbeitszeiterfassung inkl. Abwesenheiten
- Tätigkeitserfassung inkl. Kunden-/Projektverwaltung
- Spesenverwaltung
- Rechnungsstellung vom Anbieter an den Auftraggeber

Übersicht Art und Zweck:

		Verwendungs**zweck** in timesaver für			
Datenart (**Fett** = Muss-Felder, kursiv = optionale Fleder)	**Kategorie**	Arbeitszeiterfassung inkl. Abwensenheit	Tätigkeitserfassung inkl. Kunden-/Projektverwaltung	Spesenverwaltung	Rechnungsstellung vom Anbieter an den Auftraggeber
Personenstammdaten (**Name**, **Vorname**, *Personalcode/-nummer; NFC-ID, API-Key*) einschliesslich Kontaktdaten (**E-Mailadresse**) Onlinekennungen (*Cookie-Kennung, IP-Adresse*)	Mitarbeiter des Auftraggebers	x	x	x	
Besonders schützenswerte Daten (*Abwesenheitsdaten «Arbeitsunfähig/Krank»*)	Mitarbeiter des Auftraggebers	x			
Kundendaten von Kunden des Auftraggebers einschliesslich Kontaktdaten (**Kundenname**, *E-Mailadresse*)	Kunden des Auftraggebers		x	(x) optional, falls Spesen für Kunden erfasst werden)	
Vertragsdaten vom Auftraggeber einschliesslich Kontaktdaten (*Name, postalisch Anschrift, E-Mailadresse*)	Auftraggeber				x

Löschung, Sperrung und Berichtigung von Daten:

Anfragen zur Löschung, Sperrung und Berichtigung sind schriftlich und unter Angabe von ausreichenden Identifikationsinformationen an den Auftraggeber zu richten. Der Auftraggeber wird sich bemühen, diese Anfragen innerhalb eines angemessenen Zeitraums und in Übereinstimmung mit den geltenden gesetzlichen Bestimmungen zu bearbeiten. Bitte beachten Sie, dass die Bearbeitungszeit abhängig von der Komplexität der Anfrage variieren kann. Im Übrigen gelten die Regelungen des Vertrags.

5 Rechte und Pflichten des Anbieters

Der Anbieter bestätigt, dass ihm die Vorschriften gemäss DSG und DSGVO bekannt sind. Er stellt die Einhaltung der entsprechenden Grundsätze sicher und verpflichtet sich insbesondere zur Einhaltung der Bestimmungen nach Art. 19-24 DSG; Art. 28-36 DSGVO.

Der Anbieter und ihm unterstellte Personen verarbeitet Daten von betroffenen Personen ausschliesslich wie im Rahmen des Auftrages und der Weisungen des Auftraggebers vereinbart; ausser es liegt ein gesetzlich geregelter Ausnahmefall vor, z.B. zur Offenlegung von Daten gegenüber Behörden. Der Anbieter informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstösst. Der Anbieter darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

Der Anbieter führt für die von ihm durchgeführten Bearbeitungstätigkeiten ein Verzeichnis.

Der Anbieter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Massnahmen gemäss Art. 8 DSG; Art. 32 DSVGO zum angemessenen Schutz der Daten des Auftraggebers treffen, die den jeweiligen gesetzlichen Anforderungen genügen. Der Anbieter hat technische und organisatorische Massnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Bearbeitung 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.

Die vom Anbieter getroffenen Massnahmen werden in Anhang 1 näher beschrieben. Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Anbieter gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

Der Anbieter unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen hinsichtlich der Rechte der betroffenen Personen gemäss Art. 28 f. , Art. 30 Abs. 2 Bst. b, Art. 32 Abs. 1, Art. 32 Abs. 2 Bst. c, DSG; Art. 16 bis 20 DSGVO sowie Art. 32 bis 36 DSGVO.

Der Anbieter gewährleistet, dass es den mit der Bearbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Anbieter tätigen Personen untersagt ist, die Daten ausserhalb der Weisung zu verarbeiten. Ferner gewährleistet der Anbieter, dass sich die zur Bearbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort. Der Anbieter trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen sensibilisiert, angeleitet und überwacht werden.

Der Anbieter unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der Daten des Auftraggebers bekannt werden. Der Anbieter 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.

Der Anbieter gewährleistet, seinen jeweiligen datenschutzrechtlichen Pflichten nachzukommen, ein Verfahren zur regelmässigen Überprüfung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Bearbeitung einzusetzen.

Der Anbieter 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 Datenbearbeitung nicht möglich, übernimmt der Anbieter 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.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmassnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

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.

Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person im Zusammenhang mit der Auftragsverarbeitung, verpflichtet sich der Anbieter den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

Leistungen nach Ziffer 5, 7, 8 (z.B. Herausgabe von Datenträgern, Ansprache von Betroffenen, Prüfungen) sind dem Anbieter gemäss seiner aktuellen Stundensätze bzw. externer Aufwände zu vergüten.

Der Anbieter nennt dem Auftraggeber den folgenden Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen: Der Datenschutzbeauftragte der openconcept AG, datenschutz@timesaver.ch.

6 Rechte und Pflichten des Auftraggebers

Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmässigkeit der Datenweitergabe an den Anbieter sowie für die Rechtmässigkeit der Datenbearbeitung allein verantwortlich. Insbesondere, wenn besonders schützenswerte Daten in timesaver erfasst und bearbeitet werden (z.B. Abwesenheit «Arbeitsunfähig/Krank»).

Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden.

Der Auftraggeber hat den Anbieter unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmässigkeiten bzgl. Datenschutzrechtlicher Bestimmungen feststellt.

Der Auftraggeber nennt dem Anbieter den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen, sofern dieser von den durch den Auftraggeber bereits benannten Ansprechpartnern (Benutzer mit Adminstrationsrecht) abweicht. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Person sind dem Anbieter Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

Der Auftraggeber erklärt, dass er die alleinige Verantwortung trägt für die Information der von der Datenverarbeitung betroffenen Personen betreffend der möglichen Datenspeicherung, -nutzung, -bearbeitung durch den Anbieter gemäss den Bestimmungen in den AGB, der DSE und diesem AVV. Sollten einzelne betroffene Personen mit der vorgesehenen Datenbearbeitung nicht einverstanden sein, ist der Auftraggeber verantwortlich die jeweiligen Daten in timesaver entsprechend zu löschen.

7 Anfragen betroffener Personen

Wendet sich ein Dritter oder eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Anbieter, wird der Anbieter den Dritten oder die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber möglich ist. Der Anbieter leitet den Antrag des Dritten oder der betroffenen Person innerhalb eines Zeitraums von maximal 24 Stunden an den Auftraggeber weiter. Der Anbieter unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Anbieter ist in diesem Fall berechtigt, eine Aufwandsentschädigung zu verlangen. Der Anbieter haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

8 Nachweismöglichkeiten

Der Anbieter weist dem Auftraggeber die Einhaltung der in dieser Anlage niedergelegten Pflichten mit geeigneten Mitteln nach. Dies erfolgt durch einen Selbstaudit und/oder Zertifizierung gemäss ISO 27001.

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 Anbieter 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 Anbieter stehen, hat der Anbieter gegen diesen ein Einspruchsrecht.

Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich der vorangehende Absatz in Kapitel 8 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.

9 Subunternehmer (weitere Anbieter)

Die Beauftragung von Subunternehmern durch den Anbieter ist zulässig, soweit diese im Umfang des Unterauftrags ihrerseits die Anforderungen der vorliegenden Anlage erfüllen. Eine Liste der aktuellen Subunternehmer sind hier aufgelistet:

- Google Cloud EMA Limited → Zweck: Analysetool

Der Auftraggeber stimmt zu, dass der Anbieter Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Anbieter den Auftraggeber. Der Anbieter ist verpflichtet den Auftraggeber über die Beauftragung eines Subunternehmers durch Aktualisierung der eben genannten Übersicht zu informieren. Die Übersicht welche mindestens 14 Tage vorab der geplanten Änderung zu aktualisieren ist. Der Auftraggeber wird regelmässig die Übersicht einsehen. Der Auftraggeber kann der Änderung – innerhalb dieser 14 Tage – aus wichtigem Grund – gegenüber dem Anbieter 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 Anbieter ein Sonder-kündigungsrecht eingeräumt.

Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Anbieter weitere Anbieter mit der ganzen oder einer Teilleistung der in dieser Anlage vereinbarten Leistung beauftragt. Der Anbieter wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informations-sicherheitsmassnahmen zu gewährleisten. Subunternehmer, welche keine Zugriff auf Kundendaten haben bzw. keine Bearbeitung von Kundendaten vornehmen, sind von dieser Ziffer ausgenommen und werden entsprechend nicht in der genannten Liste erscheinen.

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

10 Informationspflichten

Sollten die Daten des Auftraggebers beim Anbieter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Massnahmen Dritter gefährdet werden, so hat der Anbieter den Auftraggeber unverzüglich darüber zu informieren. Der Anbieter 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 Datenschutz-Grundverordnung liegen.

11 Haftung

Die Haftung richtet sich nach dem Vertrag.

12 Sonstiges

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.

Anhang 1 ist wesentlicher Bestandteil dieser Anlage.

Anhang 1 - Technische und organisatorische Massnahmen

Die nachfolgenden technischen und organisatorischen Massnahmen sind grundlegend für die Datenbearbeitung

Zutrittskontrolle:

Es existieren folgende Massnahmen zur Zutrittskontrolle:

1. Festlegung von Sicherheitsbereichen
2. Realisierung eines wirksamen Zutrittsschutzes (Automatische Zutrittskontrolle)
3. Festlegung zutrittsberechtigter Personen
4. Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus
5. Begleitung von Besuchern und Fremdpersonal

Zugangskontrolle:

1. Zugangsschutz (Authentisierung)
2. Einfache Authentisierung der Mitarbeiter (per Benutzername/Passwort und IP-Adresse)
3. Festlegung befugter Personen
4. Verwaltung und Dokumentation von Zugangsberechtigungen
5. Manuelle Zugangssperre
6. Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk
7. Protokollierung des Zugangs

Zugriffskontrolle:

Es existieren folgende Massnahmen zur Zugriffskontrolle:

1. Erstellen eines Berechtigungskonzepts
2. Umsetzen von Zugriffsbeschränkungen
3. Vergabe minimaler Berechtigungen
4. Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen

Transport- / Weitergabekontrolle:

Es existieren folgende Massnahmen zur Weitergabekontrolle:

1. Sichere Datenübertragung zwischen Server und Client (https:)
2. Sichere Datenübertragung von Backups (https:)
3. Implementation von Sicherheitsgateways an den Netzübergabepunkten
4. Härtung der Backendsysteme
5. Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder
6. Maschine-Maschine Authentisierung

Verfügbarkeitskontrolle:

Es existieren folgende Massnahmen zur Verfügbarkeitskontrolle:

1. Backup-Konzept
2. Notfallplan
3. Aufbewahrung der Backups (in 2. Rechenzentrum an einem anderen Standort und im Datenschutztresor)
4. Prüfung der Notfalleinrichtungen

Trennungsgebot:

Es existieren folgende Massnahmen zur Verwendungszweckkontrolle:

1. Sparsamkeit bei der Datenerhebung
2. Getrennte Bearbeitung

openconcept AG, September 2024