Anlage Auftragsverarbeitung zu den Allgemeinen Geschäftsbedingungen

Vereinbarung

zwischen

dem Kunden

–Auftraggeber–

und

bexio AG

Alte Jonastrasse 24

8640 Rapperswil

Schweiz

–Provider–

über die Auftragsverarbeitung.

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem zwischen den Parteien geschlossenen Vertrag (Allgemeinen Geschäftsbedingungen des Providers) 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

(1) Einzelheiten in Bezug auf die Dienstleistung des Providers sind in dem jeweiligen Vertrag zwischen Provider und Auftraggeber (nachfolgend „Vertrag“) geregelt, dieser Vertrag besteht aus den Allgemeinen Geschäftsbedingungen des Providers.

(2) Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung, sofern in Anhang A nichts Abweichendes aufgeführt ist.

(3) Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

2 Anwendungsbereich und Verantwortlichkeit

(1) Der Provider verarbeitet die in Anhang A genannten Daten im Auftrag des Auftraggebers zu dem dort genannten Zweck in dem genannten Umfang. Dies umfasst Tätigkeiten, die im Vertrag konkretisiert sind.

(2) 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.

(3) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Provider bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform durch den Auftraggeber nachzuholen.

3 Pflichten des Providers

(1) 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 solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) 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.

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

(4) Der Provider unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen sowie bei der Einhaltung der datenschutzrechtlichen Pflichten.

(5) 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.

(6) 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.

(7) Der Provider nennt dem Auftraggeber den folgenden Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen: Der Datenschutzbeauftragte der bexio AG, datenschutz@bexio.com.

(8) Der Provider gewährleistet, seinen jeweiligen datenschutzrechtlichen Pflichten nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

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.

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.

(9) 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.

(10) 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.

(11) Leistungen nach Ziffer 3, 5, 6(2) und 6(3) (z.B. Herausgabe von Datenträgern, Ansprache von Betroffenen, Prüfungen) sind dem Provider gemäß seiner aktuellen Stundensätze bzw. externer Aufwände zu vergüten.

4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Provider unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) 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

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

(1) Der Provider 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.

(2) 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.

(3) 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)

(1) Die Beauftragung von Subunternehmern durch den Provider ist zulässig, soweit diese im Umfang des Unterauftrags ihrerseits die Anforderungen der vorliegenden Anlage erfüllen. Eine Liste der aktuellen Subunternehmer ist hier abrufbar:
https://www.bexio.com/de-CH/richtlinien/subunternehmer

(2) 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.

(3) 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 keine Zugriff auf Kundendaten haben bzw. keine Bearbeitung von Kundendaten vornehmen, sind von diesem Kapitel ausgenommen und werden entsprechend nicht in der genannten Liste erscheinen.

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

8 Informationspflichten

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. 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 Datenschutz-Grundverordnung liegen.

9 Haftung

Die Haftung richtet sich nach dem Vertrag.

10 Sonstiges

(1) 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.

(2) Anhang A und B sind wesentlicher Bestandteil dieser Anlage.

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 (Auftragsverwaltung, Kontaktverwaltung (CRM), Buchhaltung, E-Banking, Lohnbuchhaltung, Lagerverwaltung, Projektverwaltung).
Art der personenbezogenen Daten:	Die Datenarten hängen von den durch den Auftraggeber übermittelten Daten ab. Diese sind (abhängig vom Auftrag): • Personenstammdaten (Name, Geburtsdatum, Anschrift, Arbeitgeber) einschließlich Kontaktdaten (z.B. Telefon, E-Mail) • Vertragsdaten, einschließlich Abrechnung und Zahlungsdaten • Historie der Vertragsdaten
Kategorien betroffener Personen:	Die Kategorien der betroffenen Personen hängen von den durch den Auftraggeber übermittelten Daten ab. Diese sind (abhängig vom Auftrag): • Mitarbeiter (einschließlich Bewerber und ehemaligen Mitarbeitern) des Auftraggebers, • Kunden des Auftraggebers • Interessenten des Auftraggebers • Dienstleister 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

Zum Vertrag zur Auftragsdatenverarbeitung

Technische und organisatorische Maßnahmen (TOM)

1 Technische und organisatorische Maßnahmen

Die nachfolgenden technischen und organisatorischen Maßnahmen (kurz TOM) sind grundlegend für die Datenverarbeitung

(1) Zutrittskontrolle:

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

1) Festlegung von Sicherheitsbereichen
2) Realisierung eines wirksamen Zutrittsschutzes
3) Festlegung zutrittsberechtigter Personen
4) Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus
5) Begleitung von Besuchern und Fremdpersonal
6) Überwachung der Räume außerhalb der Schließzeiten
7) Protokollierung des Zutritts

(2) Zugangskontrolle:

1) Zugangsschutz (Authentisierung)
2) Einfache Authentisierung der Mitarbeiter (per Benutzername/Passwort) bei hohem Schutzniveau
3) Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
4) Verbot Speicherfunktion für Passwörter und/oder Formulareingaben
5) Festlegung befugter Personen
6) Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen
7) Automatische Zugangssperre
8) Manuelle Zugangssperre
9) Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk
10) Protokollierung des Zugangs

(3) 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
5) Protokollierung des Datenzugriffs

(4) Transport- / Weitergabekontrolle:

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

1) Sichere Datenübertragung zwischen Server und Client
2) Sicherung der Übertragung im Backend
3) Sicherung der Übertragung zu externen Systemen

4) Implementation von Sicherheitsgateways an den Netzübergabepunkten
5) Härtung der Backendsysteme
6) Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder
7) Maschine-Maschine Authentisierung
8) Datenträgerverwaltung (Verfahren)
9) Prozess zur Sammlung und Entsorgung
10) Datenschutzgerechtes Lösch-/ Zerstörungsverfahren

(5) Eingabekontrolle:

Es existieren folgende Maßnahmen zur Eingabekontrolle:

1) Dokumentation der Eingabeberechtigungen
2) Protokollierung der Eingaben

(6) Auftragskontrolle:

Es existieren folgende Maßnahmen zur Eingabekontrolle:

3) Dokumentation der Eingabeberechtigungen
4) Protokollierung der Eingaben

(7) Verfügbarkeitskontrolle:

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

1) Backup-Konzept
2) Notfallplan
3) Aufbewahrung der Backups
4) Prüfung der Notfalleinrichtungen

(8) Trennungsgebot:

Es existieren folgende Maßnahmen zur Verwendungszweckkontrolle:

1) Sparsamkeit bei der Datenerhebung
2) Getrennte Verarbeitung