Auftragsverarbeitungsvertrag

bexio AG

Dieser Auftragsverarbeitungsvertrag (nachfolgend "AVV") konkretisiert die Verpflichtungen betreffend Datenschutz, welche sich aus dem Vertragsverhältnis zwischen der bexio AG (nachfolgend "Provider") und ihren Kundinnen und Kunden (nachfolgend "Auftraggeber") ergeben. Grundlage für das Vertragsverhältnis der Parteien bilden die Allgemeinen Geschäftsbedingungen (nachfolgend "AGB") und die Datenschutzerklärung (nachfolgend "DSE") und diese sind somit integrierender Bestandteil des AVV. Der AVV findet Anwendung auf alle Tätigkeiten, die sich aus dem Vertragsverhältnis der Parteien ergeben und bei denen Mitarbeitende des Providers oder durch den Provider beauftrage Dritte personenbezogene Daten (nachfolgend "Daten") des Auftraggebers verarbeiten. Für sämtliche anfallende Datenschutzfragen kann der Auftraggeber den Datenschutzbeauftragen des Providers über datenschutz@bexio.com erreichen.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1. Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung ergeben sich grundsätzlich aus den AGB, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen ergeben.

1.2. Im Anhang A zum AVV werden Gegenstand, Art und Zweck der Auftragsverarbeitung spezifiziert.

2. Anwendungsbereich und Verantwortlichkeit

2.1. Der Provider verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in den AGB, der DSE, im Anhang A des AVV und in der aktuellen Leistungsbeschreibung auf der Website des Providers konkretisiert sind.

2.2. Der Auftraggeber ist im Rahmen des Vertragsverhältnisses 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.

2.3. Durch Ausfüllen der Anmeldemaske zur Registrierung und Bestellung eines Benutzerkontos ("bexio-Konto") auf der Website des Providers erteilt der Auftraggeber dem Provider die entsprechende Weisung zur Datenverarbeitung. Der Auftraggeber kann seine Weisungen in seinem bexio-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 oder durch entsprechende Vornahme im bexio-Konto durch den Auftraggeber nachzuholen.

3. Pflichten des Providers

3.1. Der Provider verarbeitet Daten von betroffenen Personen nur im Rahmen des Vertragsverhältnisses gemäss den AGB, der DSE und dem vorliegenden AVV; ausser es liegt ein gesetzlich geregelter Ausnahmefall vor.

3.2. 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 Daten des Auftraggebers, die den jeweiligen gesetzlichen Anforderungen genügen. Insbesondere stellen diese die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicher. 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.

3.3. Die vom Provider getroffenen Massnahmen werden in Anhang B präzisiert. Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Provider gestattet, alternative adäquate Massnahmen jederzeit umzusetzen. Dabei darf das mit diesem AVV vertraglich vereinbarte Sicherheitsniveau nicht unterschritten werden.

3.4. Der Provider unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der datenschutzrechtlichen Anfragen und Ansprüche betroffener Personen sowie bei der Einhaltung der datenschutzrechtlichen Pflichten. Der Provider ist gemäss AGB berechtigt, hierfür eine Aufwandsentschädigung zu verlangen.

3.5. Die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitenden sowie weitere für den Provider tätige Dritte verarbeiten die Daten ausschliesslich im Rahmen des Vertragsverhältnisses gemäss den AGB, der DSE und dem vorliegenden AVV und sind zur Geheimhaltung verpflichtet.

3.6. Sofern dem Provider Verletzung des Schutzes personenbezogener Daten bekannt werden, trifft er die zumutbaren Massnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen. Ausserdem hält der Provider die geltenden gesetzlichen Bestimmungen betreffend Meldung von Verletzungen des Datenschutzes vollumfänglich ein.

3.7. Der Provider hält die geltenden datenschutzrechtlichen Bestimmungen vollumfänglich ein und überprüft die Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung regelmässig.

3.8. Der Provider bearbeitet und speichert personenbezogene Daten, solange das Vertragsverhältnis zwischen dem Provider und dem Auftraggeber besteht. Der Provider berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Davon ausgenommen sind Daten, welche für die Weiterbearbeitung aufgrund gesetzlicher Vorschriften oder für zwingende interne Zwecke erforderlich sind. Die Herausgabe der Daten und die entsprechende Vergütung ist in den AGB geregelt.

4. Pflichten des Auftraggebers

4.1. Der Auftraggeber hat den Provider unverzüglich und vollständig schriftlich oder über das bexio-Konto zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmässigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4.2. Der Auftraggeber nennt dem Provider den Ansprechpartner für im Rahmen des Vertragsverhältnisses anfallende Datenschutzfragen, sofern dieser von der genannten Ansprechperson abweicht.

4.3. Der Kunde erklärt, dass er die alleinige Verantwortung trägt für die Information der von der Datenverarbeitung betroffenen Personen betreffend der möglichen Datenspeicherung, -nutzung, -bearbeitung und -weitergabe durch den Provider 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 seinem bexio-Konto entsprechend zu löschen.

4.4. Mit Akzeptierung der AGB sowie der DSE erklärt der Auftraggeber **ausdrücklich sein Einverständnis zur Weitergabe seiner Daten an die Muttergesellschaft des Providers** sowie verbundene Gesellschaften. Der Auftraggeber befreit den Provider von jeglichen möglichen Ansprüchen. Die Einholung des Einverständnisses der betroffenen Personen ist Sache des Auftraggebers.

5. Anfragen betroffener Personen

5.1. 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 innert angemessener Frist an den Auftraggeber weiter. Der Provider kann den Auftraggeber bei datenschutzrechtlichen Ansprüchen einer betroffenen Person im Rahmen seiner Möglichkeiten unterstützen. Der Provider ist in diesem Fall berechtigt, eine Aufwandsentschädigung zu verlangen. Der Provider haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6. Nachweismöglichkeiten

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

6.2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein (z.B. aufgrund Unterstellung DSGVO), 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, kann der Provider diesen ablehnen und eine neutrale Person vorschlagen. Allfällige mit der Prüfung verbundene Kosten kann der Provider dem Auftraggeber in Rechnung stellen, insbesondere wenn keine Unregelmässigkeiten festgestellt werden konnten.

6.3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Ziffer 6.2 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)

7.1. Der Provider kann zur Erfüllung der vertraglichen Leistung Subunternehmer beiziehen. Die Beauftragung von Subunternehmern als Auftragsverarbeiter durch den Provider ist zulässig, soweit diese im Umfang des Unterauftrags ihrerseits die Anforderungen des vorliegenden AVV erfüllen. Der Provider trifft mit den Subunternehmern im erforderlichen Umfang

Vereinbarungen, um angemessene Datenschutz- und Informationssicherheitsmassnahmen zu gewährleisten. Subunternehmer, welche keinen Zugriff auf Kundendaten haben bzw. keine Verarbeitung von personenbezogenen Daten als Auftragsverarbeiter vornehmen, sind von diesem Kapitel ausgenommen. Eine Liste der aktuellen Subunternehmer im Sinne eines Auftragsverarbeiters (nachfolgend einfachheitshalber nur "Subunternehmer") ist hier abrufbar: https://www.bexio.com/de-CH/richtlinien/subunternehmer

7.2. Der Auftraggeber stimmt zu, dass der Provider die auf der Website des Providers genannten Subunternehmer hinzuzieht. Vor Hinzuziehung weiterer Subunternehmer informiert der Provider den Auftraggeber durch Aktualisierung seiner Website. Die Übersicht auf der Website ist jeweils mindestens 14 Tage vor Hinzuziehung zu aktualisieren. Der Auftraggeber wird regelmässig die Übersicht einsehen. Der Auftraggeber kann der Änderung innert 14 Tagen seit Kenntnisnahme aus wichtigem Grund 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.

8. Informationspflichten

8.1. 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 liegen.

9. Haftung

9.1. Die Haftung richtet sich nach den entsprechenden Bestimmungen in den AGB.

10. Sonstiges

10.1. Im Übrigen gelten die Bestimmungen in den AGB und DSE. Bei etwaigen Widersprüchen zwischen dem AVV und den AGB gehen die Bestimmungen in den AGB vor. Sollten einzelne Teile des AVV unwirksam sein, so berührt dies die Wirksamkeit der AGB und der übrigen Bestimmungen des AVV nicht.

Anhang A und B sind wesentlicher Bestandteil des AVV.

Letzte Version: Juni 2022

bexio AG

Alte Jonastrasse 24
8640 Rapperswil
Schweiz

Anhang A Gegenstand, Art und Zweck
Anhang B Technische und organisatorische Massnahmen (TOM)

Anhang A – Gegenstand, Art und Zweck

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 gemäss den AGB und dem entsprechenden Leistungsbeschrieb auf der Website des Providers (Auftragsverwaltung, Kontaktverwaltung (CRM), Buchhaltung, E-Banking, Lohnbuchhaltung, Lagerverwaltung, Projektverwaltung, etc.).
Art der personenbezogenen Daten:	Die Datenarten hängen von den durch den Auftraggeber übermittelten Daten ab. Diese sind insbesondere (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 insbesondere (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 in den AGB, in der DSE und dem vorliegenden AVV.

Anhang B - Technische und organisatorische Massnahmen (TOM)

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

I. Zutrittskontrolle:

- Festlegung von Sicherheitsbereichen
- Realisierung eines wirksamen Zutrittsschutzes
- Festlegung zutrittsberechtigter Personen
- Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus
- Überwachung der Räume ausserhalb der Schliesszeiten
- Protokollierung des Zutritts

II. Zugangskontrolle:

- Zugangsschutz (Authentisierung)
- Einfache Authentisierung der Mitarbeiter (per Benutzername/Passwort) bei hohem Schutzniveau
- Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
- Festlegung befugter Personen
- Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen
- Automatische Zugangssperre
- Manuelle Zugangssperre
- Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk
- Protokollierung des Zugangs

III. Zugriffskontrolle:

- Erstellen eines Berechtigungskonzepts
- Umsetzen von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
- Protokollierung des Datenzugriffs

IV. Transport- / Weitergabekontrolle:

- Sichere Datenübertragung zwischen Server und Client
- 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
- Datenträgerverwaltung (Verfahren)
- Prozess zur Sammlung und Entsorgung
- Datenschutzgerechtes Lösch-/ Zerstörungsverfahren

V. Eingabekontrolle:

- Automatische Dokumentation der Eingabeberechtigungen
- Protokollierung der Eingaben

VI. Auftragskontrolle:

- Dokumentation der Eingabeberechtigungen
- Protokollierung der Eingaben

VII. Verfügbarkeitskontrolle:

- Backup-Konzept
- Notfallplan
- Aufbewahrung der Backups
- Prüfung der Notfalleinrichtungen

VIII. Trennungsgebot:

- Sparsamkeit bei der Datenerhebung
- Getrennte Verarbeitung