Vereinbarung zur Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:

(im Folgenden Auftraggeber)

Der Auftragsverarbeiter:

everii Austria GmbH
Mariahilfer Straße 121b/7.OG
A-1060 Wien

(im Folgenden Auftragnehmer)

1. Gegenstand der Vereinbarung

1.1. Der Gegenstand der Auftragsdatenverarbeitung ist in Grundsätzen im bestehenden Lizenzvertrag / Wartungsvertrag / Softwarenutzungsvertrag beschrieben. Der Auftrag enthält jedenfalls die Installation, den Betrieb, die Wartung sowie den Support der TEAMBOX. Diese Vereinbarung ist als Ergänzung zum Hauptvertrag im Hinblick auf die Erfüllung der Bestimmungen der DSGVO zu verstehen. Durch diese Vertragsergänzung wird der Leistungsinhalt des Hauptvertrages daher nicht verändert, sondern lediglich DSGVO konform konkretisiert.

1.2. Folgende Datenkategorien werden verarbeitet:
- Stammdaten
- Kontaktdaten
- Arbeitsaufzeichnungen
- Projektdaten
- Verrechnungsdaten
- Bestelldaten
- Protokolldaten

1.3. Folgende Kategorien betroffener Personen unterliegen der Datenverarbeitung:
- Kunden
- Geschäftspartner / Lieferanten
- New Business / Potentialkunden

und Ansprechpartner der angegebenen Kategorien sowie Mitarbeiter

2. Dauer der Vereinbarung

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung. Eine Beendigung dieser Vereinbarung unabhängig vom Hauptvertrag ist nicht vorgesehen.

3. Pflichten des Auftragnehmers

3.1. Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

3.2. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

3.3. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind dem Anhang Technisch-organisatorische Maßnahmen zu entnehmen).

3.4. Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

3.5. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation). In diesem Zusammenhang anfallende Leistungen werden nach Aufwand verrechnet.

3.6. Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

3.7. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen des Auftragsnehmers, sei es auch durch von ihm beauftragte Dritte, eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

3.8. Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder in einem anderen, gängigen Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat herauszugeben.

3.9. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. Technisch-organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.
Einzelheiten sind dem Anhang zu entnehmen.

5. Ort der Durchführung der Datenverarbeitung

Alle Datenverarbeitungstätigkeiten werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in der Schweizerischen Eidgenossenschaft durchgeführt.

Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Datenschutzniveau ergibt sich aus:

- einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO.
- einer Ausnahme für den bestimmten Fall nach Art 49 Abs 1 DSGVO.
- verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Abs 2 lit b DSGVO.
- Standarddatenschutzklauseln nach Art 46 Abs 2 lit c und d DSGVO.
- genehmigten Verhaltensregeln nach Art 46 Abs 2 lit e iVm Art 40 DSGVO.
- einen genehmigten Zertifizierungsmechanismus nach Art 46 Abs 2 lit f iVm Art 42 DSGVO.
- von der Datenschutzbehörde bewilligte Vertragsklauseln nach Art 46 Abs 3 lit a DSGVO.
- einer Ausnahme für den Einzelfall nach Art 49 Abs 1 Unterabsatz 2 DSGVO.

6. Sub-Auftragsverarbeiter

6.1. Der Auftragnehmer kann Sub-Auftragsverarbeiter zur unmittelbaren Erbringung der Hauptdienstleistung hinzuziehen. Aktuell sind das folgende Sub-Auftragsnehmer:

Name	Adresse	Land	Kurzbeschreibung
everii Switzerland AG	Albisriederstrasse 253 8047 Zürich	Schweiz	Tochterunternehmen für Kundenbetreuung/Support
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen	Deutschland	Hosting
Hubspot Inc.	25 First Street, Cambridge, MA 02492	USA	Support, Kommunikation und Online-Hilfen Datenstandort: EU

Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer dies dem Auftraggeber eine angemessene Zeit vorab schriftlich anzeigt und
- der Auftraggeber nicht gegenüber dem Auftragnehmer schriftlich Einspruch gegen die geplante Auslagerung erhebt.

Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 2-4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

6.2. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.3. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/ des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

7. Weisungsbefugnis des Auftraggebers

7.1. Weisungen des Auftraggebers betreffend Datenschutz relevante Tätigkeiten sind an den Auftragnehmer bzw. dessen Mitarbeiter grundsätzlich schriftlich, zumindest jedoch per E-Mail zu richten.

7.2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber so geändert ist, dass Datenschutzkonformität hergestellt ist.

8. Datenschutzbeauftragter des Auftragnehmers

8.1. PROLIANCE GmbH
Leopoldstraße 21
80802 München
www.datenschutzexperte.de
datenschutzbeauftragter@datenschutzexperte.de

9. Sonstiges

Mit der Übersendung dieses Vereinbarungstexts bietet der Auftragnehmer den Abschluss der Vereinbarung in der vorliegenden Form an. Die Vereinbarung kommt daher mit der Unterschrift des Auftraggebers gültig zustande.

_____, am _____

Für den Auftraggeber:

_____
Name und Funktion

Wien, am

Für den Auftragnehmer:

_____
Martin Reitbauer-Ortner, Geschäftsführer

Anlage
Technisch-organisatorische Maßnahmen (TOMs)

Im Folgenden werden die Technisch-organisatorischen Maßnahmen des Auftragnehmers beschrieben. Software-as-a-Service Installationen der TEAMBOX (nur bei Wahl der Installationsart ‚TEAMBOX.as-a-service' relevant) werden auf Rootservern der Sub-Auftragsverarbeiter gehostet, die für angemessene TOMs sorgen.

Vertraulichkeit

Zutrittskontrolle

- Der Zugang zu den Büroräumlichten und dem Serverraum erfolgt über jeweils individualisierte und protokollierte Schließanlage.
- Die Büroräumlichkeiten sind mit einer Alarmanlage inkl. externer Alarmierung einer Sicherheitsfirma gesichert.

Zugangskontrolle

- Der Zugang zu Servern und Services erfolgt über individualisierte und authentifizierte Benutzerkonten.
- Der Zugriff auf Arbeitsplatzrechner ist mittels Passwort geschützt.

Zugriffskontrolle

- Zugriffskontrolle erfolgt durch rollenbasierte Freigabe von Berechtigungen für spezifische Usergruppen.
- Der Zugriff auf Kundendaten ist auf den Anlassfall beschränkt (Installation, Wartung, Support).
- Alle Zugriffe auf Kundendaten werden protokolliert.

Integrität

Weitergabekontrolle

- Die Zugriffe auf Datenanwendungen erfolgen unter Transportverschlüsselung, auch im internen Netz.
- Sämtliche Datenträger, die extern verwendet werden, sind verschlüsselt.
- Alle Arbeitsplatzrechner sind mit Passwort geschützt und mit verschlüsselter Festplatte ausgestattet.

Eingabekontrolle

- Die Verarbeitung (Eingabe/Veränderung/Verarbeitung) von personenbezogenen Daten in unseren Systemen wird protokolliert und nur von jeweils berechtigten Mitarbeitern vorgenommen.

Verfügbarkeit und Belastbarkeit

- Es sind USV Anlagen für sämtliche Server vorhanden.
- Die Internetzugang ist über Firewall gesichert.
- Es erfolgen tägliche Backups sowohl der Server als auch der Arbeitsplatzrechner. Dadurch ist eine rasche Wiederherstellung gewährleistet.
- Die SaaS-Installationen der TEAMBOX werden täglich lokal und auf einem Backupserver in einem separaten Rechenzentrum eines Hostingpartners gesichert. Damit ist eine einfache Wiederherstellung gewährleistet.
- Im Fall der Vertragsauflösung werden die Daten des Kunden sofort gelöscht.
- Alle Zugänge von ausgetretener Mitarbeiter werden sofort deaktiviert.
- Verwendete Betriebssysteme / Anwendungen / Firmware werden regelmäßig upgedatet.
- Ein Monitoring der Verfügbarkeit ist implementiert.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management

- Die Mitarbeiter sind zum Datenschutz geschult und haben eine gesonderte Verpflichtungserklärung zu Datenschutz und Verschwiegenheit unterschrieben.
- Information von Mitarbeitern zum Verhalten beim Eintreten eines Datenschutzvorfalls sind dokumentiert und geschult.
- Die TEAMBOX verfügt über datenschutzfreundliche Voreinstellungen.

Auftragskontrolle

- Die Auftragsdatenverarbeitung erfolgt Aufgrund des bestehenden Lizenzvertrag / Wartungsvertrag / Softwarenutzungsvertrag und der ergänzenden Vereinbarung zur Auftragsverarbeitung.
- Der Zugriff auf personenbezogen Daten des Auftraggebers erfolgt ausschließlich im Supportfall. Dabei wird ein nachvollziehbarer Auftrag in Form eines Tickets im Aufgabenkontrollsystem angelegt und verfolgt.