Auftragsdatenbearbeitungsvereinbarung / Auftragsverarbeitungsvertrag (ADV/AVV) · Data Processing Agreement (DPA)

Hinweis: Diese Auftragsverarbeitungsvereinbarung (AVV) wird durch Bezugnahme Bestandteil des zwischen dem Verantwortlichen und der Auftragsverarbeiterin abgeschlossenen Hauptvertrags. Eine gesonderte Unterzeichnung dieser AVV ist nicht erforderlich.

Dokumentinformationen

Bezeichnung:	Auftragsdatenbearbeitungsvereinbarung / Auftragsverarbeitungsvertrag (ADV/AVV) · Data Processing Agreement (DPA)
Version:	2607
Autor(en):	Michael Ammann / Boxalino AG

Inhaltsverzeichnis

Auftragsdatenbearbeitungsvereinbarung

zwischen

dem jeweiligen Kunden, nachfolgend «Auftraggeber» genannt,

und

Boxalino AG, Hertistrasse 27a, 8304 Wallisellen, nachfolgend «Auftragsbearbeiter» genannt,

einzeln «Partei» und gemeinsam «Parteien» genannt.

Präambel

A. Die Parteien haben eine Vereinbarung betreffend eine vom Auftragsbearbeiter zur Verfügung gestellte SaaS-Plattform abgeschlossen (die «SaaS-Vereinbarung») und darin die Erbringung verschiedener Leistungen vereinbart (die «Dienstleistungen»).

B. Im Rahmen der SaaS-Vereinbarung stellt der Auftraggeber dem Auftragsbearbeiter Personendaten zur Verfügung.

C. Um die Einhaltung der datenschutzrechtlichen Anforderungen bei der Bearbeitung von Personendaten durch den Auftragsbearbeiter sicherzustellen, schliessen die Parteien die vorliegende Auftragsdatenbearbeitungsvereinbarung (die «Vereinbarung»).

Dies vorausgeschickt, vereinbaren die Parteien was folgt:

1. Vertragsgegenstand

1.1. Gegenstand

Die Parteien regeln in dieser Vereinbarung nur das datenschutzrechtliche Auftragsbearbeitungsverhältnis. Sie beabsichtigen nicht, den in der SaaS-Vereinbarung vereinbarten Leistungskatalog auszuweiten oder einzuschränken.

1.2. Konfliktregelung

Bei Widersprüchen zwischen Vertragsbestimmungen gilt die folgende Rangfolge: Die Anhänge dieser Vereinbarung gehen der Vereinbarung vor, und die SaaS-Vereinbarung geht dieser Vereinbarung vor.

1.3. Definitionen

Fettgedruckte Begriffe werden in dieser Vereinbarung jeweils mit der ihnen zugewiesenen Bedeutung verwendet. Rechtsbegriffe wie «Personendaten», «Bearbeitung» usw. haben die im anwendbaren Datenschutzrecht festgelegte Bedeutung.

2. Gegenstand und Dauer der Auftragsbearbeitung

2.1. Auftragsbearbeitung

Der Auftragsbearbeiter bearbeitet im Zusammenhang mit den Dienstleistungen Personendaten im Auftrag des Auftraggebers (die «Auftragsdaten»). Der Gegenstand der Auftragsbearbeitung, ihre Art und ihr Zweck ergeben sich aus der SaaS-Vereinbarung. Die Kategorien der von der Auftragsbearbeitung betroffenen Personen und die Kategorien der betroffenen Personendaten werden in Anhang 1 beschrieben.

2.2. Weitere Dienstleistungen

Soweit der Auftragsbearbeiter im Lauf der Zusammenarbeit weitere Dienstleistungen für den Auftraggeber übernimmt, gilt diese Vereinbarung auch für diese Dienstleistungen.

2.3. Dauer

Diese Vereinbarung beginnt mit dem Inkrafttreten des Hauptvertrags (SaaS-Vereinbarung), spätestens aber mit dem ersten Zugriff des Auftragsbearbeiters auf Auftragsdaten. Sie endet mit Beendigung der SaaS-Vereinbarung.

2.4. Stellung des Auftraggebers

Der Auftraggeber ist sich bewusst, dass die gesetzliche Verantwortung für die Zulässigkeit der Erhebung und Bearbeitung der Auftragsdaten und für die Erfüllung der Betroffenenrechte im Zusammenhang mit den Dienstleistungen bei ihm liegt.

3. Pflichten des Auftragsbearbeiters

3.1. Befolgung von Weisungen

a) Der Auftragsbearbeiter ist verpflichtet, die Auftragsdaten ausschliesslich für die Dienstleistungen zu verwenden und bei ihrer Bearbeitung die Weisungen des Auftraggebers zu befolgen. Vorbehalten sind abweichende Pflichten des anwendbaren Rechts (z.B. verbindliche Anordnungen zuständiger Behörden), über die der Auftraggeber soweit zulässig zu informieren ist. Das Weisungsrecht wird durch die SaaS-Vereinbarung und durch diese Vereinbarung beschränkt.

b) Die Weisungen des Auftraggebers sind in Textform zu erteilen, wobei sie in dringenden Fällen auch mündlich erteilt werden können.

3.2. Verzeichnis von Verarbeitungstätigkeiten

Der Auftragsbearbeiter verpflichtet sich, in Bezug auf die Auftragsdaten ein Verzeichnis von Verarbeitungstätigkeiten gemäss anwendbarem Datenschutzrecht zu führen. Der Auftragsbearbeiter wird dem Auftraggeber auf Anfrage jederzeit Einblick in dieses Verzeichnis gewähren.

3.3. Ort der Datenbearbeitung

Die Bearbeitung und Nutzung der Auftragsdaten finden grundsätzlich in der Schweiz sowie der EU statt. Einige der Unterauftragnehmer gemäss Anhang 3 bearbeiten gewisse Auftragsdaten gegebenenfalls für Spezialfunktionen auch ausserhalb der Schweiz und der EU. Diese sind, falls zutreffend, im Anhang 3 ausdrücklich aufgeführt.

3.4. Rückgabe- und Löschpflicht

a) Nach Beendigung der Vereinbarung hat der Auftragsbearbeiter die Auftragsdaten zu löschen. Datenlöschungen müssen jeweils endgültig erfolgen, und auf Anfrage ist dem Auftraggeber die Löschung zu bestätigen.

b) Ist der Auftragsbearbeiter aufgrund gesetzlicher Vorschriften zur Aufbewahrung von Auftragsdaten gesetzlich verpflichtet, hat er den Auftraggeber frühzeitig entsprechend zu informieren.

4. Datensicherheit

4.1. Sicherheitsmassnahmen

Der Auftragsbearbeiter ergreift angemessene, in jedem Fall aber mindestens die in Anhang 2 umschriebenen technischen und organisatorischen Massnahmen zum Schutz der Auftragsdaten (die «Sicherheitsmassnahmen»). Der Auftragsbearbeiter ist während der Dauer der Vereinbarung berechtigt, die Sicherheitsmassnahmen anzupassen, sofern dabei das Sicherheitsniveau nicht abgesenkt wird, und ist zur Anpassung verpflichtet, soweit dies für die Aufrechterhaltung des Schutzniveaus gemäss dem anwendbaren Datenschutzrecht erforderlich ist.

4.2. Meldung von Verletzungen

a) Bei konkret festgestellten Sicherheitsverletzungen, die zur Vernichtung, zum Verlust, zur Veränderung oder zur Offenlegung von Personendaten führen, informiert der Auftragsbearbeiter den Auftraggeber unverzüglich, spätestens aber innert 24 Stunden.

b) Der Auftragsbearbeiter ist verpflichtet, dem Auftraggeber auf Anfrage weitere sachdienliche Auskünfte zur Sicherheitsverletzung zu erteilen, soweit dies ohne Verletzung seiner vertraglichen und gesetzlichen Geheimhaltungspflichten möglich ist.

5. Unterauftragnehmer

5.1. Zulässigkeit

a) Für die Erbringung der Dienstleistungen ist der Auftragsbearbeiter befugt, nach freiem Ermessen Unterauftragnehmern Auftragsdaten zur Verfügung zu stellen, sofern der Auftragsbearbeiter die Vorgaben gemäss dieser Ziff. 5 einhält. Als Unterauftragnehmer im Sinne dieser Vereinbarung gilt jeder Dienstleister, dessen Leistungen sich unmittelbar auf die Bearbeitung von Auftragsdaten beziehen.

b) Der Auftragsbearbeiter hat mit den betroffenen Unterauftragnehmern Vereinbarungen zu treffen, die mindestens ebenso strenge Regelungen enthalten wie die vorliegende Vereinbarung.

c) Der Auftragsbearbeiter ist dafür verantwortlich, dass die Unterauftragnehmer die Auftragsdaten konform mit den anwendbaren Gesetzen bearbeiten.

d) Der Auftragsbearbeiter ist zur Gewährleistung des Datenschutzes und der Datensicherheit verpflichtet, angemessene und regelmässige Kontrollmassnahmen bei den betroffenen Unterauftragnehmern zu ergreifen. Sofern diese Kontrollmassnahmen zeigen sollten, dass ein oder mehrere Unterauftragnehmer die Auftragsdaten nicht konform mit den anwendbaren Gesetzen bearbeiten, wird er den Auftraggeber proaktiv informieren.

e) Der Auftragsbearbeiter wird den Auftraggeber auf dessen Anfrage über seine Tätigkeiten gemäss dieser Ziff. 5.1 informieren.

5.2. Genehmigung

a) Eine Liste der bei Vertragsbeginn bestehenden und hiermit genehmigten Unterauftragnehmer mit Zugriff auf Auftragsdaten findet sich in Anhang 3. Vor einer Änderung eines Unterauftragnehmers wird der Auftraggeber darüber informiert. Erklärt der Auftraggeber nicht innerhalb von 20 Kalendertagen ab Zugang der entsprechenden Mitteilung, dass er mit der Änderung nicht einverstanden ist, gilt der betreffende Unterauftragnehmer als genehmigt.

b) Bei rechtzeitiger Ablehnung des Unterauftragnehmers verständigen sich die Parteien über eine Alternative. Sofern die Parteien nicht innerhalb von 30 Kalendertagen nach der Ablehnung durch den Auftraggeber eine Einigung erzielen, ist jede Partei berechtigt, die SaaS-Vereinbarung zu kündigen.

5.3. Unterauftragnehmer ausserhalb der Schweiz und der EU

Sofern Auftragsdaten im Zusammenhang mit dem erlaubten Beizug eines Unterauftragnehmers in einen Staat ohne angemessenes Datenschutzniveau gelangen bzw. von dort zugänglich sind, ist der Auftragsbearbeiter vor der ersten Bekanntgabe von Auftragsdaten an den betreffenden Unterauftragnehmer verpflichtet, geeignete Garantien in Übereinstimmung mit dem anwendbaren Datenschutzrecht (z.B. die anwendbaren EU-Standardvertragsklauseln) einzuholen.

5.4. Dokumentation

Auf Anfrage übermittelt der Auftragsbearbeiter dem Auftraggeber eine Kopie mit den relevanten Teilen seiner Vereinbarung(en) mit Unterauftragnehmern (ggf. einschliesslich der geeigneten Garantien), damit der Auftraggeber die Einhaltung dieser Vereinbarung durch den Auftragsbearbeiter prüfen kann.

5.5. Haftung

Der Auftragsbearbeiter haftet dem Auftraggeber für die Einhaltung der Pflichten der Unterauftragnehmer gemäss den Bestimmungen der SaaS-Vereinbarung.

6. Prüfrechte

6.1. Prüfrecht

Der Auftraggeber hat das Recht, jederzeit die Einhaltung der gesetzlichen und vertraglichen Pflichten im Zusammenhang mit dieser Vereinbarung durch den Auftragsbearbeiter und/oder dessen Unterauftragnehmer zu prüfen, maximal aber einmal pro Kalenderjahr. Der Auftragsbearbeiter ist verpflichtet, bei Prüfungen jeweils angemessen mitzuwirken. Sämtliche Prüfungen sind vorab mit dem Auftragsbearbeiter abzustimmen. Der Auftraggeber nimmt bei der Planung und Durchführung der Prüfung Rücksicht auf die Bedürfnisse und Sicherheitsanforderungen des Auftragsbearbeiters und hat Vertraulichkeitsverpflichtungen des Auftragsbearbeiters zu respektieren.

6.2. Externe Prüfstelle

Der Auftraggeber hat das Recht, die Prüfung gemäss Ziff. 6.1 vorstehend durch eine externe, fachkundige und zur Vertraulichkeit verpflichtete Person durchführen zu lassen. Die Kosten der externen Prüfstelle nach dieser Ziff. 6.2 trägt der Auftraggeber.

7. Unterstützungspflichten

7.1. Datensicherheit

Der Auftragsbearbeiter unterstützt den Auftraggeber in angemessener Weise bei der Einhaltung seiner gesetzlichen Pflichten zur Gewährleistung einer angemessenen Datensicherheit und zur Meldung von Datenschutzverletzungen sowie bei der Durchführung von Datenschutz-Folgenabschätzungen.

7.2. Betroffenenrechte

Soweit sich eine betroffene Person im Zusammenhang mit datenschutzrechtlichen Ansprüchen (z.B. mit einem Auskunfts- oder Löschbegehren) an den Auftragsbearbeiter wendet und diese Ansprüche mit den Dienstleistungen zusammenhängen, leitet der Auftragsbearbeiter das entsprechende Begehren unverzüglich dem Auftraggeber weiter. Er unterstützt den Auftraggeber angemessen bei der Bearbeitung solcher Begehren.

7.3. Informationspflicht

Kontrollhandlungen und andere Massnahmen von Datenschutzaufsichtsbehörden sind dem Auftraggeber unverzüglich zu melden (soweit zulässig), wenn sie die Auftragsdaten oder für die Bearbeitung von Auftragsdaten verwendete Systeme betreffen.

7.4. Kontakt

Für datenschutzrechtliche Themen ist beim Auftragsbearbeiter in erster Linie folgende Person zu kontaktieren: Sylvain Paillard, +41 43 210 33 63, Sylvain.Paillard@boxalino.com.

8. Vertraulichkeit

8.1. Auftragsdaten

Der Auftragsbearbeiter verpflichtet sich, Auftragsdaten strikt vertraulich zu behandeln und innerhalb und ausserhalb seiner Organisation nur Personen zugänglich zu machen, die für die Erfüllung ihrer Pflichten auf Zugang zu den Auftragsdaten angewiesen sind. Er stellt sicher, dass alle Personen mit Zugang zu Auftragsdaten mit Bezug auf diese einer gesetzlichen oder vertraglichen Vertraulichkeitspflicht unterstehen.

8.2. Sonstige Informationen

Beide Parteien unterstehen zudem mit Bezug auf im Rahmen dieser Vereinbarung wahrgenommene Tatsachen den auf sie anwendbaren gesetzlichen und zwischen ihnen in der SaaS-Vereinbarung vereinbarten Vertraulichkeitspflichten.

9. Schlussbestimmungen

9.1. Haftung

Für die Haftung aus Verletzungen dieser Vereinbarung gelten die entsprechenden Bestimmungen der SaaS-Vereinbarung.

9.2. Mitteilungen

In dieser Vereinbarung vorgesehene Mitteilungen müssen jeweils ausdrücklich und in Textform (z.B. per E-Mail oder Post) erfolgen, sofern nichts anderes vereinbart ist.

9.3. Die Anhänge dieser Vereinbarung sind integrierte Bestandteile derselben.

9.4. Änderungen und Ergänzungen

Änderungen und Ergänzungen dieser Vereinbarung erfolgen durch eine neue, im Hauptvertrag bezeichnete Version dieser Vereinbarung oder durch schriftliche Vereinbarung der Parteien.

9.5. Streitschlichtung

Das anwendbare Recht und der Gerichtsstand richten sich nach der SaaS-Vereinbarung.

9.6. Inkrafttreten

Diese Auftragsverarbeitungsvereinbarung tritt mit dem wirksamen Abschluss des Hauptvertrags in Kraft, sofern dieser auf die jeweils gültige Fassung dieser AVV verweist. Mit der Annahme des Hauptvertrags erkennen beide Vertragsparteien diese AVV als verbindlichen Vertragsbestandteil an.

9.7. Versionierung

Es gilt die zum Zeitpunkt des Vertragsabschlusses unter der im Hauptvertrag bezeichneten URL veröffentlichte Version dieser AVV.

9.8. Verhältnis zum Hauptvertrag

Diese AVV bildet einen integrierenden Bestandteil des Hauptvertrags zwischen den Parteien. Soweit diese AVV wirksam in den Hauptvertrag einbezogen wurde, entfaltet sie dieselbe rechtliche Verbindlichkeit wie der Hauptvertrag selbst.

Anhang 1 — Konkretisierung der Vereinbarung

Gegenstand, Art und Zweck der Vereinbarung

Im Einzelnen sind insbesondere die folgenden Daten Bestandteile der Datenverarbeitung:

(a) Art und Zweck der Datenverarbeitung:
Der Auftragnehmer betreibt die Echtzeitplattform (Plattform) «Winning Interactions» zum Datenmanagement, sowie der Analyse des Nutzerverhaltens und der Echtzeitoptimierung von Online-Shops, Smartphone Apps, Portalen (Channels) usw. Diese Plattform beinhaltet auch ein Data-Warehouse und erlaubt es Anwendern, beliebige ergänzende Daten zu verwalten und zu bearbeiten. Die Plattform zeichnet unter anderem auch das Verhalten von Nutzern der Online-Shops, Apps usw. auf und speichert diese Verhaltensdaten zur Analyse und Verarbeitung und Optimierung der Channels.

(b) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen Kunden/Interessenten und weitere Personen des Auftraggebers wie:

- Online-Shop / Portal Nutzer
- E-Mail-Empfänger
- ggf. weitere Personen die per Datenexport zur Plattform übermittelt werden

(c) Datenarten und -kategorien
Die betroffenen Datenarten ergeben sich aus nachfolgender Aufzählung:

Leistung	Kategorien von Personendaten	Betroffene Personen
(Echtzeit-) Optimierung von E-Touchpoints (Online-Shops, E-Mail etc.)	Persönliche Daten (z.B. Namen, Adresse, etc.); Kaufverhalten (z.B. Online und POS-Transaktionen); Reaktionen auf Kommunikation (z.B. E-Mail); Verhaltensdaten (z.B. Sessions, Requests, IP-Adresse im E-Shop)	Kunden und nicht-identifizierte Besucher des Online-Shops; ggf. Mitarbeiter
Kommunikations-Optimierung, Bereitstellung Datenfeeds	Persönliche Daten (z.B. Namen, Adresse, etc.); Kaufverhalten (z.B. Online und POS-Transaktionen); Reaktionen auf Kommunikation (z.B. E-Mail); Verhaltensdaten (z.B. Sessions, Requests, IP-Adresse im E-Shop)	Kunden und nicht-identifizierte Besucher des Online-Shops; ggf. Mitarbeiter
Data Mining, Analytics, Reporting	Persönliche Daten (z.B. Namen, Adresse, etc.); Kaufverhalten (z.B. Online und POS-Transaktionen); Reaktionen auf Kommunikation (z.B. E-Mail); Verhaltensdaten (z.B. Sessions, Requests, IP-Adresse im E-Shop)	Kunden und nicht-identifizierte Besucher des E-Shops; ggf. Mitarbeiter

Anhang 2 — Beschreibung der technischen und organisatorischen Massnahmen (TOM)

Im Folgenden werden die technischen und organisatorischen Massnahmen beschrieben, die der Auftragnehmer im Zusammenhang mit der Bearbeitung von Personendaten und der Erfüllung seiner Verpflichtungen im Rahmen der bestehenden Verträge und Art. 32 DSGVO, soweit diese anwendbar ist, trifft:

Zutrittskontrolle

Massnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

- **Realisierung des Zutrittsschutzes:**
  - Der zu schützende Bereich ist durch eine geeignete Bauweise abgesichert.
  - Alle möglichen Zugänge wurden gegen unbefugten Zugang gesichert.
  - Es besteht eine für alle verbindliche Zugangs-Authentisierung (Schlüssel oder Chipkarte).
- **Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen:**
  - Es gibt organisatorische Regelungen über Zutrittsberechtigungen zum Geschäftsbereich.
  - Es gibt eine Dokumentation über die Vergabe der Schlüssel.

Zugangskontrolle

Massnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (einschliesslich Verschlüsselungsverfahren):

- **Zugangsschutz (Authentisierung):**
  - Es besteht Zugangsschutz zu allen Datenverarbeitungssystemen durch Benutzer-Authentisierung.
  - Die Umsetzung der Massnahmen zum Zugangsschutz wird kontrolliert.
  - Es wird ein Passwort-Generator für Zufalls-Passwörter genutzt.
- **Gesicherte Übertragung von Authentisierungs-Geheimnissen (Credentials) im Netzwerk:**
  - Die Übertragung der Authentisierungs-Geheimnisse über das Netz erfolgt verschlüsselt.
  - Es existiert ein sicheres Verfahren zur Rücksetzung nach Zugangssperren, z.B. Neuvergabe einer Nutzerkennung.
- **Verbot der lokalen Speicherung für Passworte und/oder Formulareingaben:**
  - Zugriffspasswörter und/oder Formulareingaben werden nicht auf dem Client selbst oder in seiner Umgebung abgelegt (z.B. Speicherung im Browser oder Haftnotizen).
  - Ausgenommen ist die lokale Speicherung in speziell dafür vorgesehenen Anwendungen (e.g. Passwort-Safes).
  - Die Nutzer werden über diese Vorgaben belehrt.

- **Festlegung befugter Personen:**
  - Der Kreis der befugten Personen ist auf das betriebsnötige Minimum reduziert.
- **Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen:**
  - Für die Vergabe von Zugangsberechtigungen ist eine verantwortliche Person benannt.
- **Automatische Zugangssperre:**
  - Bei mehr als 30 Minuten Inaktivität einer Arbeitsstation bzw. eines Terminals wird ein kennwortgeschützter Bildschirmschoner mit Hilfe der betriebssystemeigenen Mechanismen automatisch aktiviert.
- **Manuelle Zugangssperre:**
  - Es existiert eine Richtlinie, Arbeitsstationen und Terminals bei vorübergehendem Verlassen des Arbeitsplatzes gegen unbefugte Nutzung zu schützen, z.B. durch automatische oder manuelle Aktivierung des kennwortgeschützten Bildschirmschoners.
  - Die Mitarbeiter werden hinsichtlich der Notwendigkeit der Umsetzung dieser Massnahmen geschult.

Zugriffskontrolle

Massnahmen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (einschliesslich Verschlüsselungsverfahren):

- **Berechtigungskonzept/Umsetzung von Zugriffsbeschränkungen:**
  - Es gibt Regelungen zum Anlegen, Ändern und Löschen von Berechtigungsprofilen.
- **Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen:**
  - Entfällt die Grundlage für eine Berechtigung (z.B. durch Funktionsänderung), wird diese sofort entzogen.

Weitergabekontrolle

Massnahmen, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (einschliesslich Verschlüsselungsverfahren):

- **Sichere Datenübertragung zwischen Server und Client:**
  - Die Datenübertragung zwischen Clients und Servern erfolgt verschlüsselt (SSL, SSH, SFTP oder VPN).
- **Übertragung im Backend:**
  - Die Verbindung zu den Backendsystemen ist geschützt.

- **Härtung der Backend-Systeme:**
  - Voreingestellte Dienstkonten/Passworte wurden deaktiviert.
- **Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder:**
  - Es gibt eine dokumentierte Schnittstellenspezifikation.
  - Eine Versendung von personenbezogenen Daten per Post findet nicht statt.
- **Prozess zur Sammlung und Entsorgung:**
  - Es existieren Regelungen zur datenschutzkonformen Vernichtung von Datenträgern.
  - Es existieren Regelungen zur datenschutzkonformen Vernichtung von Dokumenten.
- **Datenschutzgerechtes Lösch-/Zerstörungsverfahren:**
  - Datenträger werden vor Wiederbenutzung durch andere Nutzer datenschutzgerecht gelöscht; eine Wiederherstellung der gelöschten Daten ist gar nicht oder nur mit unverhältnismässigem Aufwand möglich.
  - Hardwarekomponenten oder Dokumente werden so vernichtet, dass eine Wiederherstellung gar nicht oder nur mit unverhältnismässigem Aufwand möglich ist.

Auftragskontrolle

Massnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle):

- **Ausübung der Kontrollpflichten:**
  - Der Auftragnehmer unterstützt den Auftraggeber bei der Ausübung seiner Kontrollpflichten.
  - Alle auftretenden Vorfälle werden dem Auftraggeber gemeldet.
  - Der Auftragnehmer hat alle Mitarbeiter über die Meldepflicht von Vorfällen informiert.

Verfügbarkeitskontrolle

Massnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle):

- **Backup-Konzept:**
  - Es existiert ein Backup-Konzept.
  - Backups finden regelmässig statt.
  - Eine für das Backup verantwortliche Person und Vertreter sind benannt.
- **Notfallplan:**
  - Es existiert ein Notfallplan, in dem die einzuleitenden Schritte aufgeführt werden und in dem festgelegt ist, welche Personen, insbesondere auch auf Seiten des Auftraggebers, über den Vorfall zu unterrichten sind.

Zweckbindung

Massnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Die Daten unterschiedlicher Kunden des Auftragnehmers werden in getrennten Tabellen, Dateien und in getrennten Verzeichnissen gespeichert und nicht zusammengeführt.

Organisationskontrolle

- **Prozessdefinition/-kontrolle:**
  - Es gibt Verfahrensanweisungen.
  - Für die Verarbeitung von Daten im Unternehmen sind Prozesse und Arbeitsabläufe definiert.
  - Die Umsetzung und Einhaltung der Prozesse werden kontrolliert.
- **Schulung/Verpflichtung:**
  - organisatorischer Massnahmen.
  - Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse einschliesslich den Vorgängen des Auftraggebers.
  - Ordnungsgemässer und sorgfältiger Umgang mit Daten, Dateien, Datenträgern und sonstigen Unterlagen.
  - Die Schulungen sind dokumentiert.
  - Die Schulungen werden regelmässig wiederholt, mindestens jedoch alle drei Jahre.

Anpassungen und Änderungen

Eine Änderung der getroffenen Sicherheitsmassnahmen bleibt dem Auftragnehmer vorbehalten, wobei sichergestellt werden muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

Weitere Sicherheitsmassnahmen können in der SaaS-Vereinbarung geregelt werden.

Anhang 3 — Genehmigte Unterauftragnehmer

Die folgenden Personen gelten zum Zeitpunkt des Vertragsabschlusses als Unterauftragnehmer im Sinne dieser Vereinbarung. Hinweis: bei Google nutzen wir EU Multiregional als Data-Center.

Name und Sitz	**Betroffene Dienstleistungen**	**Aufgabe(n) des Unterauftragnehmers**
Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA	«Winning Interactions» Plattform Betrieb	Traffic Management, Server-less Funktionen und weitere Dienste
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland	«Winning Interactions» Plattform Betrieb	Virtuelle und reale Server Infrastruktur inkl. Netzwerkmanagement
Hosttech GmbH, Seestrasse 15a, 8805 Richterswil, Schweiz	«Winning Interactions» Plattform Betrieb	Virtuelle und reale Server Infrastruktur inkl. Netzwerkmanagement
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	«Winning Interactions» Plattform Betrieb	Big Data Storage & Processing, Analytics & Reporting, Notifikationen usw.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA	Support / Helpdesk	Datenaustausch, E-Mail
InterVenture Sourcing AG, Sihlquai 125, 8005 Zürich, Switzerland	Data Science Service auf Basis der «Winning Interactions» Plattform	Data Science Services
Slack Technologies, Inc., Slack Legal Department, 500 Howard Street, San Francisco, California 94105, USA	Support / Weisungen	Bereitstellung des Slack Instant Messangers
Twilio Inc., San Francisco, USA	«Winning Interactions» Plattform Betrieb	E-Mail Versand und weitere Services
Zendesk, 1019 Market St., San Francisco, CA 94103, USA	Support / Helpdesk	Verwaltung von Support-Tickets
Zoom Video Communications, Inc., 55 Almaden Blvd, Suite 600, San Jose, CA 95113, USA	Support / Helpdesk	Videoconferencing

Boxalino AG
Hertistrasse 27a
8304 Wallisellen / Zürich
Switzerland

CHE-101.628.584
michael.ammann@boxalino.com

+41 43 210 33 63 (Telefon)

www.winning-interactions.ai