Auftragsverarbeitungsvertrag

gem. Art 28 ff Datenschutz-Grundverordnung ("DSGVO“)

Version 02.02.2023

Auftragsverarbeiterin:

baningo GmbH
Sechskrügelgasse 2/7
1070 Wien
Österreich

1. Präambel

1. Die baningo GmbH (nachfolgend Auftragnehmerin), verarbeitet auf Grundlage dieses Auftragsverarbeitungsvertrages (nachfolgend AVV) personenbezogene Daten im Sinne des Art 4 Z 1 Datenschutz-Grundverordnung (DSGVO) für Ihre Kunden (nachfolgend “Auftraggeberin”).
2. Dieser Vertrag ergänzt unsere Allgemeinen Geschäftsbedingungen (AGB) und bildet die vertragliche Basis für die Auftragsdatenverarbeitung im Sinne des Art 28 Abs 3 DSGVO. Bei Widersprüchen geht dieser Vertrag den AGB vor und ist geltungserhaltend im Sinne der DSGVO und der begleitenden Datenschutzgesetze auszulegen.
3. Die Auftragnehmerin stellt der Auftraggeberin mit baningo cards eine Software-Lösung für digitale Visitenkarten zur Verfügung. Hierbei werden Mitarbeiterdaten der Auftraggeberin verarbeitet. Abhängig von den verwendeten Funktionen durch die Auftraggeberin, kann es zur Verarbeitung von Kundendaten der Auftraggeberin kommen.

2. Vertragsgegenstand

1. Die Auftragsnehmerin als Auftragsverarbeiter iSd Art 4 Z 8 DSGVO verarbeitet die personenbezogenen Daten im Auftrag der Auftraggeberin als Verantwortliche im Rahmen ihrer Tätigkeit(en).
2. Diese Vereinbarung umfasst sämtliche personenbezogene Daten (Art 4 Z 1 DSGVO),
    a. welche die Auftragnehmerin für die Auftraggeberin in Erfüllung ihrer vertraglichen Verpflichtungen aus dem Servicevertrag verarbeitet oder
    b. auf welche die Auftragnehmerin Zugriff nimmt oder nehmen kann, auch wenn sie nicht ausdrücklich in der Beilage 1 angeführt sind.

3. Rechte und Pflichten der Auftraggeberin

1. Die Auftraggeberin erklärt ausdrücklich, für die vertragsgegenständlichen personenbezogenen Daten „Verantwortlicher" im Sinne des Art 4 Z 7 DSGVO zu sein. Alleine die Auftraggeberin entscheidet daher im Rahmen des Vertragsverhältnisses der Vertragsparteien über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten.
2. Die Auftraggeberin ist ua dafür verantwortlich, dass für die Verarbeitung personenbezogener Daten, mit der der Auftragsverarbeiter beauftragt wird, eine ausreichende Rechtsgrundlage besteht und für die Zulässigkeit der Verarbeitung der personenbezogenen Daten für Einhaltung der DSGVO und der begleitenden Datenschutzgesetze und die Gewährung der Betroffenenrechte zu sorgen.
3. Deshalb steht der Auftraggeberin auch ein datenschutzrechtliches Weisungsrecht zu, in welcher Form und in welchem Umfang die personenbezogenen Daten von der Auftragnehmerin zu verarbeiten sind; sofern Weisungen der Auftraggeberin gegen das Datenschutzrecht verstoßen, trifft den Auftragnehmer eine Hinweispflicht (Art 28 Abs 3 3. Satz DSGVO). Offensichtlich rechtswidrige Weisungen sind von der Auftragnehmerin nicht zu befolgen.

4. Alleine die Auftraggeberin ist daher berechtigt, über die Verwendung, Löschung und Berichtigung von personenbezogenen Daten zu entscheiden.
5. Im Sinne der Transparenz tritt alleine die Auftraggeberin gegenüber Dritten als Verantwortlicher in Erscheinung.

4. Art und Umfang der Datenverarbeitung

1. Die personenbezogenen Daten sind von der Auftragnehmerin
    a. ausschließlich zum Zwecke der Erfüllung der vertraglichen Verpflichtungen gegenüber der Auftraggeberin zu verwenden;
    b. nicht für eigene oder fremde Zwecke zu verwenden;
    c. ausschließlich der Auftraggeberin zurückzugeben und nur nach schriftlichem Auftrag an Dritte zu übermitteln;
    d. innerhalb des räumlichen Geltungsbereiches der DSGVO zu verarbeiten, sofern die Auftraggeberin dem nicht ausdrücklich schriftlich zustimmt;
    e. so zu verarbeiten, dass die Auftraggeberin jederzeit in der Lage ist, ihre datenschutzrechtlichen Pflichten gegenüber Betroffenen und Aufsichtsbehörden zu erfüllen.
2. Jeglicher Verstoß gegen die Art und den Umfang der Datenverarbeitung durch die Auftragnehmerin führt dazu, dass sie selbst als Verantwortlicher für die unrechtmäßige Datenverarbeitung einzustehen hat (Art 28 Abs 10 DSGVO).

5. Pflichten der Auftragnehmerin

1. Die Auftragnehmerin ist im Umfang der übernommenen vertraglichen Verpflichtungen für die ordnungsgemäße Auftragsdatenverarbeitung im Rahmen des Servicevertrages und der bestehenden Datenschutzgesetze verantwortlich.
2. Verpflichtungen, die sich nicht bereits aus dem Servicevertrag oder dem objektiven Recht ergeben, sind als „Anweisungen zur Datenverarbeitung“ in Beilage 3 dieser Vereinbarung gesondert ausgewiesen. Diese können von der

Auftraggeberin jederzeit angepasst werden. Die Auftragnehmerin trifft die Pflicht zur ordnungsgemäßen Dokumentation von derartigen Weisungen der Auftraggeberin (Art 28 Abs 3 lit a DSGVO).

3. Die Auftragnehmerin verpflichtet sich, dass sie alle zur Verarbeitung der personenbezogenen Daten befugten Personen zur Wahrung des Datengeheimnisses im Sinne des § 6 DSG und Art 28 Abs 3 lit b DSGVO verpflichtet hat, oder diese einer angemessenen, insbesondere gesetzlichen, Verschwiegenheitsverpflichtung unter-liegen (Art 28 Abs 3 lit b DSGVO).
4. Ausdrücklich sagt die Auftragnehmerin zu, dass diese befugten Personen zu den Themen Datenschutz, Datensicherheit und Vertraulichkeit nachweislich insbesondere zur Einhaltung datenschutzrechtlicher Bestimmungen und Prinzipien von DSGVO und der Bestimmungen dieser Vereinbarung geschult und instruiert wurden. Die Verschwiegenheitsverpflichtung hat bereits vor Aufnahme der Datenverarbeitung für die Auftraggeberin zu bestehen und auch nach Beendigung der Tätigkeit unbefristet weiterzubestehen. Die Verpflichtung zur Verschwiegenheit ist auch für Daten von juristischen Personen einzuhalten.
5. Die Auftragnehmerin verpflichtet sich ferner, alle gemäß Art 32 DSGVO erforderlichen technischen-organisatorischen Maßnahmen zu ergreifen, um die Sicherheit der Datenverarbeitung gewährleisten zu können (Art 28 Abs 3 lit c DSGVO). Die Auftragnehmerin wird daher auf eigene Kosten alle organisatorischen und technischen Maßnahmen ergreifen, die ihres Erachtens erforderlich sind, um (i) die Sicherheit und Integrität der Datenverarbeitung zu gewährleisten, (ii) Verluste personenbezogener Daten zu verhüten, und (iii) den unbefugten Zugriff Dritter auf die personenbezogenen Daten zu verhindern. Die von der Auftragnehmerin zum Zeitpunkt der Unterzeichnung dieser Vereinbarung ergriffenen Maßnahmen sind in ihrem Sicherheitskonzept beschrieben und können in der Beilage 2 entnommen werden.
6. Die Auftragnehmerin verpflichtet sich, die Auftraggeberin bei der Geltendmachung von Betroffenenrechten nach besten Kräften zu unterstützen (Art 28 Abs 3 lit e DSGVO). Die Auftragnehmerin trägt insbesondere für die technischen und organisatorischen Voraussetzungen Vorsorge, dass die

Auftraggeberin ihre Verpflichtungen zum Auskunftsrecht (Art 15 DSGVO), zum Recht auf Berichtigung (Art 16 DSGVO) und zum Recht auf Löschung („Recht auf Vergessenwerden“, Art 17 DSGVO) gegenüber dem Betroffenen innerhalb der gesetzlichen Fristen jederzeit erfüllen kann. Die Auftragnehmerin überlässt der Auftraggeberin hierfür alle notwendigen Informationen.

7. Die Auftragnehmerin verpflichtet sich, die Auftraggeberin bei der Einhaltung ihrer Verpflichtungen gemäß Art 32 bis 36 DSGVO (insbesondere zur Vornahme ausreichender technisch-organisatorischer Maßnahmen, zur Datenschutzfolgeabschätzung und zur Security Breach Notification) nach besten Kräften zu unterstützen (Art 28 Abs 3 lit f DSGVO).
8. Die Auftragnehmerin ist ferner verpflichtet, die Auftraggeberin unverzüglich von jeder Verletzung der des Datenschutzes oder der Datensicherheit, insbesondere auch im Fall behördlicher Maßnahmen oder eines Insolvenzverfahrens, zu informieren.

6. Einsatz von weiteren Auftragsverarbeitern

(Art 28 Abs 2 und Abs 4 lit d DSGVO)

1. Die Auftraggeberin erteilt hiermit die allgemeine schriftliche Genehmigung gemäß Art 28 Abs 2 DSGVO, dass die Auftragnehmerin ihre vertraglichen Verpflichtungen aus dieser Vereinbarung auf andere Unternehmen („weitere Auftragsverarbeiter“) übertragen darf, sofern sie mit diesen ebenso eine Vereinbarung im Sinne des Art 28 Abs 4 DSGVO abschließt. Die Auftragnehmerin hat jedoch die Auftraggeberin von der beabsichtigten Heranziehung eines weiteren Auftragsverarbeiter so rechtzeitig zu verständigen, dass die Auftraggeberin dies im Einklang mit Art 28 Abs 2 DSGVO allenfalls untersagen kann.

   Alle weiteren Auftragsverarbeiter müssen den in dieser Vereinbarung enthaltenen Bedingungen entsprechen. Die Auftragnehmerin ist für die

Handlungen und Unterlassungen dieser Unter-Auftragsverarbeiter voll datenschutzrechtlich verantwortlich. Eine Auflistung der derzeitigen weiteren Auftragsverarbeiter ist in der Beilage 4 enthalten.

2. Weitere Auftragsverarbeiter außerhalb des EWR wird die Auftragnehmerin jedenfalls nur dann beauftragen, wenn (i) diese in einem Drittland niedergelassen sind, das über ein von der EU-Kommission mit Beschluss akzeptiertes angemessenes Datenschutzniveau verfügt (Angemessenheitsbeschluss) oder (ii) mit diesen die EU-Standardvertragsklauseln bzw diesen gleichgestellte durch die EU-Kommission erlassene Vertragsschablonen als geeignete Garantien im Sinne des Art 46 Abs 2 lit c und d DSGVO vereinbart wurden.

7. Kontrollrechte

(Art 28 Abs 3 lit h DSGVO

Die Auftragnehmerin verpflichtet sich für den Zeitraum bis 1 Jahr nach Beendigung des Servicevertrages, der Auftraggeberin auf deren Wunsch, jedoch nicht häufiger als einmal im Jahr, die Erfüllung der Bedingungen dieser Vereinbarung nachzuweisen. Dieser Nachweis betrifft insbesondere die implementierten technischen und organisatorischen Sicherheitsmaßnahmen. Ein solcher Nachweis kann aus Bestätigungen oder Zertifizierungen interner oder externer Prüfer oder des Datenschutzbeauftragten bestehen, in besonderen Fällen auch durch Inspektionen.

8. Datenschutzbeauftragter

1. Bei Vorliegen der Voraussetzungen des Art 37 DSGVO ist die Auftragnehmerin (zumindest) für die Laufzeit dieser Vereinbarung verpflichtet, einen Datenschutzbeauftragten zu bestellen.

2. Die Auftragnehmerin wird der Auftraggeberin auf deren Wunsch den Namen des jeweiligen Datenschutzbeauftragten unverzüglich mitteilen.

9. Vertragsdauer

1. Diese Vereinbarung tritt mit Unterzeichnung durch beide Vertragsparteien in Kraft und wird für die Geltungsdauer des referenzierten Servicevertrages abgeschlossen.
2. Die Auftragnehmerin ist nach Beendigung ihrer Dienstleistung verpflichtet, nach Weisung der Auftraggeberin alle Daten, Verarbeitungsergebnisse und Unterlagen zu retournieren oder auftragsgemäß zu löschen.
3. Die Verpflichtung zur Wahrung der Verschwiegenheit dauert über den Zeitraum der aufrechten Vertragsbeziehung unbefristet an.

10. Schlussbestimmungen

1. Änderungen und Ergänzungen zu diesem Vertrag bedürfen der Schriftform, was auch in einem elektronischen Format erfolgen kann. Gleiches gilt für die Vereinbarung, vom Erfordernis der Schriftform abzugehen. Die Vereinbarung einschließlich ihrer Anhänge ist von beiden Parteien schriftlich, auch elektronisch, aufzubewahren.
2. Diese Vereinbarung unterliegt materiellem österreichischen Recht unter Ausschluss der Verweisungsnormen sowie dem sachlich relevanten Unionsrecht, insbesondere der DSGVO. Gerichtsstand für Streitigkeiten zu dieser Vereinbarung ist am Sitz der Auftragnehmerin.
3. Im Übrigen gelten die Regelungen des zwischen den Vertragsparteien abgeschlossenen Servicevertrages unverändert fort.

Beilage 1: **Spezifikation der personenbezogenen Daten**

Beschreibung der Art der personenbezogenen Daten, die im Auftrag des Verantwortlichen im Sinne der zugrundeliegenden Vereinbarung zur Auftragsverarbeitung verarbeitet werden:

Daten unserer Kunden und ihrer Mitarbeiter / von unseren Kunden bekannt gegeben:	**Verpflichtend J/N**	**Kommentar**
Vorname & Nachname	J	
Akademischer Grad	N	
E-Mail-Adresse (n)	J	
Telefonnummer (n)	N	
Arbeitgeber / Unternehmen	J	
Position	N	
Adresse	J	
Geburtsdatum	N	
Lichtbild	N	
Passwort	J	
Video	N	
Hochgeladene Daten	N	
Individuelle Inhalte: z.B. Über mich, Berufserfahrung, Aus- und Weiterbildung, Kenntnisse, Moto, Credo, Produkte, Dienstleistungen, etc.	N	

Daten von Kunden unserer Kunden bekanntgegeben		
Vorname & Nachname	N	Nur falls Kontaktmodule verwendet werden
Telefonnummer	N	Nur falls Kontaktmodule verwendet werden
E-Mail-Adresse	N	Nur falls Kontaktmodule verwendet werden
Nachrichteninhalte	N	Nur falls Kontaktmodule verwendet werden
vom Verantwortlichen zusätzlich erhoben		
Access Log Einträge Webserver: - IP-Adressen - HTTP Kommunikationsprotokoll	J	Betrifft alle Zugriffe auf die Anwendung
Informationen zur Nutzung unserer Produkte (z.B. Erstelldatum von Profilen, Anzahl Logins bzw. Seitenaufrufen, Metriken bzgl. der Nutzung von Links und Kontaktoptionen, Datum des letzten Logins)	J	Diese Informationen dienen zur Analyse der Verwendung unserer Services, ermöglichen uns Verbesserungen vorzunehmen und die Sicherheit unserer Services zu überwachen und kontinuierlich zu verbessern.

Beilage 2: **Technische und organisatorische Maßnahmen**

1. Der Auftragsverarbeiter gewährleistet durch technische und organisatorische Maßnahmen, die sich nach dem Stand der Technik, den Implementierungskosten und den konkreten Risiken richten und geeignet sind, im Ergebnis ein angemessenes Schutzniveau für die Rechte der betroffenen Person sicherzustellen.

2. Der Stand der Technik bezeichnet fortschrittliche Verfahren, Einrichtungen und Betriebsweisen, die nach herrschender Auffassung sachkundiger Experten das Erreichen des gesetzlich vorgegebenen Zieles im Datenschutz gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren müssen sich in der Praxis bewährt haben und sollten möglichst im Betrieb mit Erfolg erprobt sein.

3. Die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen lassen sich wie folgt umschreiben:

(i) Zugangskontrolle

Die Einrichtungen der baningo GmbH sind mit Schließzylindern verschlossen. Schlüssel haben nur Mitarbeiter der baningo GmbH. Besucher werden stets von einem Mitarbeiter der baningo GmbH begleitet. Ausscheidenden Mitarbeitern wird der Schlüssel abgenommen. Ausgefolgte Schlüssel zu den Einrichtungen werden schriftlich dokumentiert (Schlüsselliste) und regelmäßig auf Vollständigkeit geprüft

(ii) Systemzugriffskontrolle

Die Systeme der baningo GmbH sind am Perimeter durch Firewalls, und Malware-Filter, innerhalb durch Virenscanner vor unbefugter Systembenutzung geschützt. Der Zugriff auf Systeme erfolgt mittels personengebundener Passwörter.

Gemäß internen Arbeitsanweisungen wird eine Mindestpasswortlänge und Zusammensetzung der Zeichen für alle verwendeten Systeme vorgeschrieben. Die Weitergabe oder das Teilen von Passwörtern ist strikt untersagt.

Wenn möglich ist die Verwendung von Zwei-Faktor-Authentifizierung zwingend vorgeschrieben.

(iii) Datenzugriffskontrolle

Ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems wird durch Verschlüsselung von Datenträgern und einem Zugriffsmanagement verhindert. Zugriffsberechtigungen basieren auf Rollenbeschreibungen inkl. differenzierter Berechtigungen. Diese werden regelmäßig überprüft und befugtem Personal nur in dem Ausmaß und für die Dauer eingeräumt, in dem dies zur Ausübung der Funktion der jeweiligen Person erforderlich ist („Need-to-Know" Prinzip).

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt (pseudonymisiert). Sofern es möglich ist, werden auch Verschlüsselungstechnologien zum Schutz personenbezogener Daten eingesetzt bzw. möglichst früh anonymisiert, wenn es der Zweck zulässt.

Die Zugriffe werden vom System protokolliert und sind nicht im Zugriff der Zugreifenden. Bei Datenbankzugriffen werden zwecks Nachvollziehbarkeit IP-Adresse, Zeit- und Datumsstempel protokolliert.

(iv) Weitergabekontrolle

Die baningo GmbH verwendet Schichtverschlüsselung zum Schutz von Daten, die übertragen werden. Die Kommunikation zwischen den Kundensystemen und dem System des Auftragnehmers erfolgt durch einen verschlüsselten Übertragungskanal (zB HTTPS), um die Datenübermittlung zu sichern und um durch die Verwendung von Zertifikaten und Server-Validierung Vertrauen zu schaffen.

Eine Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, erfolgt durch eine jeweils geeignete Protokollierung.

(v) Performancekontrolle

Die Systeme der baningo GmbH sind belastungsmäßig ausgeglichen und soweit möglich redundant ausgelegt. Sie basieren auf mehreren Serverstationen, die in der Lage sind einen Ausfall oder defekt zu kompensieren. Unsere Web- und Datenbankserver sind durch Firewalls abgesichert und deren Einsatz schriftlich dokumentiert. Tägliche Backups schützen vor Datenverlust von personenbezogenen Daten (Datensicherung). Nach Vertraulichkeit differenzierte Zugriffsberechtigungen schützen personenbezogene Produktivdaten zusätzlich vor zufälliger Zerstörung, Verlusten oder Missbrauch.

(vi) Evaluierungsmaßnahmen

Bei speziellen Fragestellungen holen wir uns externe Expertise ein, beispielsweise zur datenschutzkonformen Protokollierung oder datenschutzkonformen Umsetzung im Testdatenmanagement. Weiters finden regelmäßig Mitarbeiter-Schulungen mit dem Schwerpunkt Datenschutz und Informationssicherheit statt.

Beilage 3: **Weitere Auftragsverarbeiter und Übermittlungsempfänger**

Nachfolgende Tabelle enthält die von der baningo GmbH eingesetzten weiteren Auftragsverarbeiter iSd Art 28 Abs 2 DSGVO.

weitere Auftragsverarbeiter	**Zweck**
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Sitz der Gesellschaft: Deutschland Registergericht: Ansbach, HRB 6089	Rechenzentrumsbetreiber für unsere Services.
Twilio Ireland Limited 25-28 North Wall Quay Dublin 1, Ireland Sitz der Gesellschaft: Dublin, Ireland Register Nummer: IE557454, CRO ie	Versand von systemrelevanten transaktionalen E-Mails an unsere Kunden und deren Usern.

Google Dublin, Google Ireland Ltd. Gordon House, Barrow Street Dublin 4 Sitz der Gesellschaft: Irland	**Google Maps:** Dieser Service wird dafür verwendet, die Adresse auf der digitalen Visitenkarte direkt in der Google Maps Applikation zu öffnen. Hierbei werden nur die Adressdaten und keine weiteren personenbezogenen Daten an Google versendet, um einen Ausschnitt der Karte des Standortes zu erhalten. Durch nicht befüllen der Adressinformationen im Profil kann dieser Service durch den Verantwortlichen deaktiviert werden. **ReCaptcha:** Diesen Service haben wir im Sinne von Privacy per Design gem. ErG 78 umgesetzt. Das Google Recaptcha wird erst dann aktiviert, wenn mehrere Login-Versuche oder Kontaktaktionen mittels Formularen in einem definierten Zeitraum erfolgen. Diese technische Maßnahme wehrt damit gezielt Brute Force Angriffe ab und schützt somit die personenbezogenen Daten unserer Kunden. Nutzer mit „normalen“ Login Verhalten sind damit nicht von der Verarbeitung durch Google Recaptcha betroffen.

Beilage 4: **Weitere Übermittlungsempfänger**

weitere Übermittlungsempfänger	**Zweck**
Stripe Europe LTD C/O A&L GOODBODY, IFSC, NORTH WALL QUAY, DUBLIN 1, Ireland Register Nummer: IE513174	Zahlungsdienstleister für die Abrechnung unserer Services