VERTRAG ZUR AUFTRAGSVERARBEITUNG PERSONENBEZOGENER DATEN

Gemäß Artikel 28 der Verordnung (EU) 2016/679 (DSGVO) und Artikel 33 des spanischen Organgesetzes 3/2018 vom 5. Dezember über den Schutz personenbezogener Daten und die Garantie digitaler Rechte (LOPDGDD).

ZWISCHEN

Einerseits dem im Unterschriftenabschnitt dieses Dokuments identifizierten Kunden, der als Verantwortlicher (im Folgenden der „Verantwortliche“) handelt.

Und andererseits BILBAO AI, S.L., spanische USt-IdNr. B-13759758, eingetragen im Handelsregister von Bizkaia, mit Sitz in Calle Diputación 8, 4. Stock, Büro 5, 48008 Bilbao (Spanien), die als Auftragsverarbeiter (im Folgenden der „Auftragsverarbeiter“ oder „Afini.ai“) handelt. E-Mail für Datenschutzangelegenheiten: privacidad@afini.ai.

PRÄAMBEL

I. Der Verantwortliche hat die Dienste der Plattform Afini.ai (gegebenenfalls einschließlich der Produkte test.afini.ai und/oder afini.ai) zur Verarbeitung eigener oder ihm anvertrauter personenbezogener Daten beauftragt oder beabsichtigt dies.

II. Diese Verarbeitung erfordert, dass der Auftragsverarbeiter im Auftrag des Verantwortlichen auf personenbezogene Daten zugreift, was den Anwendungsbereich des Art. 28 DSGVO eröffnet.

III. Die Parteien wünschen, mit diesem Vertrag die nach geltendem Recht erforderlichen Garantien zu dokumentieren.

KLAUSELN

1. Gegenstand

Dieser Vertrag regelt die Bedingungen, unter denen der Auftragsverarbeiter im Rahmen der beauftragten Leistungen (im Folgenden die „Dienste“) personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Er ist Bestandteil des Hauptvertrags zwischen den Parteien und hat in Datenschutzfragen Vorrang vor diesem.

2. Begriffsbestimmungen

Die Begriffe „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“, „betroffene Person“, „Verletzung des Schutzes personenbezogener Daten“, „besondere Kategorien“ und „Aufsichtsbehörde“ haben die in Art. 4 DSGVO festgelegte Bedeutung. „Unter-Auftragsverarbeiter“ bezeichnet jeden vom Auftragsverarbeiter beauftragten Dritten, der im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet.

3. Laufzeit

Dieser Vertrag tritt mit Datum der letzten Unterschrift in Kraft und gilt für die Dauer der Erbringung der Dienste. Verpflichtungen, die ihrer Natur nach über die Beendigung hinaus bestehen müssen (Vertraulichkeit, Löschung, residuale Unterstützung), gelten für die gesetzlich vorgeschriebene Dauer fort.

4. Art, Zweck und Gegenstand der Verarbeitung

Der Auftragsverarbeiter verarbeitet die in Anhang I beschriebenen personenbezogenen Daten ausschließlich zum Zweck der Erbringung der Dienste an den Verantwortlichen gemäß dessen dokumentierten Weisungen, einschließlich der Erstellung kognitiver Profile, der Erstellung von Berichten und Narrativen mittels Sprachmodellen, der Rechnungsstellung und des Kundensupports. Jede weitergehende Verarbeitung zu einem anderen Zweck bedarf der vorherigen schriftlichen Anweisung des Verantwortlichen oder, andernfalls, einer eigenständigen Rechtsgrundlage.

5. Arten personenbezogener Daten und Kategorien betroffener Personen

Die Datenarten und Kategorien betroffener Personen sind in Anhang I aufgeführt. Die Verarbeitung kann besondere Kategorien gemäß Art. 9 DSGVO umfassen (psychologische Merkmale, Werte, Bindungsstile und andere aus psychometrischen Instrumenten abgeleitete Daten), sofern der Verantwortliche dies konfiguriert. Der Verantwortliche garantiert, dass eine angemessene Rechtsgrundlage für die Verarbeitung solcher Kategorien besteht.

6. Pflichten des Auftragsverarbeiters (Art. 28 Abs. 3 DSGVO)

Der Auftragsverarbeiter verpflichtet sich, (a) personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, einschließlich in Bezug auf Drittlandübermittlungen, sofern nicht eine zwingende gesetzliche Verpflichtung besteht, in welchem Fall er den Verantwortlichen vorab unterrichtet; (b) zu gewährleisten, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen; (c) alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen zu ergreifen; (d) die Bedingungen für die Inanspruchnahme von Unter-Auftragsverarbeitern gemäß Klausel 7 einzuhalten; (e) den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten zu unterstützen; (f) den Verantwortlichen bei der Einhaltung der Verpflichtungen aus den Art. 32 bis 36 DSGVO unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen zu unterstützen; (g) nach Wahl des Verantwortlichen alle personenbezogenen Daten nach Beendigung der Erbringung der Dienste zu löschen oder zurückzugeben und vorhandene Kopien zu löschen, sofern keine gesetzliche Aufbewahrungspflicht besteht; (h) dem Verantwortlichen alle für den Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten erforderlichen Informationen zur Verfügung zu stellen sowie Überprüfungen gemäß Klausel 12 zu ermöglichen und dazu beizutragen.

7. Unter-Auftragsverarbeiter (Art. 28 Abs. 2 DSGVO)

Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung zur Inanspruchnahme der in Anhang III aufgeführten Unter-Auftragsverarbeiter. Der Auftragsverarbeiter schließt mit jedem Unter-Auftragsverarbeiter einen schriftlichen Vertrag, der gleichwertige Pflichten wie dieser Vertrag auferlegt. Der Auftragsverarbeiter wird den Verantwortlichen über jede Hinzuziehung oder Ersetzung von Unter-Auftragsverarbeitern mit einer Frist von mindestens dreißig (30) Tagen über seine Datenschutzerklärung und/oder per E-Mail an die angegebene Kontaktadresse informieren und ihm die Möglichkeit zum begründeten Einspruch geben. Ein begründeter Einspruch berechtigt den

Verantwortlichen zur fristlosen Kündigung des Vertrags ohne Sanktion, wenn der Auftragsverarbeiter keine gleichwertige Alternative anbieten kann.

8. Drittlandübermittlungen (Kap. V DSGVO)

Sofern die Verarbeitung eine internationale Übermittlung außerhalb des EWR umfasst (insbesondere an Anthropic, PBC, in den USA), stützt sich der Auftragsverarbeiter auf (i) die mit dem entsprechenden Unter-Auftragsverarbeiter abgeschlossenen Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914, ergänzt gegebenenfalls durch (ii) zusätzliche technische Maßnahmen (Verschlüsselung in Transit und im Ruhezustand, Minimierung des übertragenen Inhalts) und organisatorische Maßnahmen (regelmäßige Audits, vertragliche No-Training-Klausel). Die aktuelle Übermittlungsliste findet sich in Anhang III.

9. Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Der Auftragsverarbeiter wendet die in Anhang II beschriebenen technischen und organisatorischen Maßnahmen an, die ein dem Risiko angemessenes Schutzniveau bieten. Diese Maßnahmen werden regelmäßig sowie immer dann überprüft und aktualisiert, wenn eine neue Schicht, ein neues Sprachmodell oder eine Funktion mit hoher Auswirkung eingeführt wird.

10. Verletzungen des Schutzes personenbezogener Daten (Art. 33-34 DSGVO)

Der Auftragsverarbeiter unterrichtet den Verantwortlichen über jede Verletzung des Schutzes personenbezogener Daten unverzüglich und in jedem Fall innerhalb von achtundvierzig (48) Stunden nach Kenntniserlangung. Die Meldung enthält die vernünftigerweise verfügbaren Informationen und wird mit fortschreitender Untersuchung ergänzt. Der Auftragsverarbeiter dokumentiert alle Vorfälle, ihre Auswirkungen und die ergriffenen Korrekturmaßnahmen.

11. Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen angemessen bei der Beantwortung von Anträgen betroffener Personen auf Ausübung ihrer Rechte (Auskunft, Berichtigung, Löschung, Widerspruch, Einschränkung, Datenübertragbarkeit und Recht, keiner ausschließlich automatisierten Entscheidung unterworfen zu werden). Der Auftragsverarbeiter stellt dem Verantwortlichen Dashboard-, Export- und Löschmechanismen zur Verfügung, mit denen die meisten dieser Rechte autonom erfüllt werden können.

12. Audits

Der Auftragsverarbeiter stellt dem Verantwortlichen die zur Erbringung des Nachweises der Einhaltung des Art. 28 DSGVO erforderlichen Informationen zur Verfügung, einschließlich der Executive Summary der DPIA, der Sicherheitsrichtlinie und der Zertifikate der Unter-Auftragsverarbeiter, soweit verfügbar. Der Verantwortliche kann mit angemessener Vorankündigung von mindestens sechzig (60) Tagen und höchstens einmal jährlich (außer bei schweren Vorfällen) auf eigene Kosten ein Dokumenten-Audit oder die Beantwortung eines SIG-Lite-Fragebogens verlangen. Vor-Ort-Audits bedürfen der vorherigen Zustimmung der Parteien und sind während der Geschäftszeiten ohne Beeinträchtigung des Betriebs des Auftragsverarbeiters durchzuführen.

13. Rückgabe oder Löschung nach Beendigung

Nach Beendigung der Erbringung der Dienste gibt der Auftragsverarbeiter nach schriftlicher Wahl des Verantwortlichen, die innerhalb von dreißig (30) Tagen zu treffen ist, alle personenbezogenen Daten

zurück oder löscht sie und löscht vorhandene Kopien, soweit keine gesetzliche Aufbewahrungspflicht besteht. Geht innerhalb dieser Frist keine Anweisung ein, erfolgt die Löschung von Amts wegen und wird im Verzeichnis der Verarbeitungstätigkeiten dokumentiert.

14. Haftung

Jede Partei haftet gegenüber der anderen für Schäden, die sie durch Vertragsverletzung verursacht, gemäß dem Hauptvertrag und Art. 82 DSGVO. Unbeschadet der gesamtschuldnerischen Haftung gegenüber betroffenen Personen haftet im Innenverhältnis der Auftragsverarbeiter nur, soweit er gegen die nach geltendem Recht bestehenden Pflichten verstoßen oder außerhalb oder entgegen den Weisungen des Verantwortlichen gehandelt hat.

15. Anwendbares Recht und Gerichtsstand

Dieser Vertrag unterliegt spanischem Recht und dem Recht der Europäischen Union. Die Parteien unterwerfen sich den Gerichten von Bilbao (Spanien) und verzichten ausdrücklich auf jeden anderen für sie zuständigen Gerichtsstand, soweit nicht zwingende Vorschriften entgegenstehen.

ANHANG I — BESCHREIBUNG DER VERARBEITUNG

Art und Zweck der Verarbeitung

Erbringung der Dienste der Plattform Afini.ai: Kontoverwaltung und Authentifizierung, psychometrische Bewertung (Big Five und gegebenenfalls weitere Schichten), Aufbau kognitiver Profile, Erzeugung von Berichten und Narrativen mittels Sprachmodellen, Kundensupport, Rechnungsstellung und Wartung.

Arten personenbezogener Daten

Identifikationsdaten (E-Mail, Vor- und Nachname, sofern angegeben), Nutzungsdaten des Dienstes (Anwendungsprotokolle, Nutzungsmetriken des LLM-Proxys, Audit-Ereignisse), Antworten auf psychometrische Fragebögen, Gespräche mit der KI, deklarierte Schichten des kognitiven Profils, tokenisierte Zahlungsdaten (von Stripe direkt verwaltet; der Auftragsverarbeiter speichert weder PAN noch Bankdaten).

Besondere Kategorien gemäß Art. 9 DSGVO

Bei Aktivierung durch den Verantwortlichen: psychologische Merkmale (Big Five), Humorstile (HSQ), Bindungsstile (ECR-R), persönliche Werte (AVI), Zeitorientierung (ZTPI) und sonstige aus dem kognitiv-ästhetischen Gespräch abgeleitete Daten.

Kategorien betroffener Personen

Endnutzer des Verantwortlichen, vom Verantwortlichen eingeladene Fachleute und gegebenenfalls Mitarbeiter des Verantwortlichen.

Dauer der Verarbeitung

Für die Dauer der Erbringung der Dienste sowie gegebenenfalls für die gesetzlichen Aufbewahrungsfristen.

Verarbeitungsorte

Europäische Union (Railway eu-west, Cloudflare, Sentry EU-Region) und für die LLM-Inferenz die Vereinigten Staaten (Anthropic) unter EU-Standardvertragsklauseln.

ANHANG II — TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Verschlüsselung. TLS 1.2 oder höher in Transit; AES-256 im Ruhezustand in der Datenbank und auf persistenten Volumes.

Zugangskontrolle. Starke Authentifizierung über Magic-Link und/oder OAuth, obligatorische Mehrfaktor-Authentifizierung (TOTP und WebAuthn) für Administratoren; Least-Privilege-Prinzip; periodische Rotation der Zugangsdaten und sofortige Aufhebung bei Beendigung.

Trennung der Umgebungen. Logische Trennung zwischen Entwicklungs-, Staging- und Produktivumgebungen; Geheimnisse als Umgebungsvariablen in Railway, je Service skopiert.

Nachvollziehbarkeit. Protokoll administrativer Tätigkeiten mit IP-Hash, Identität des Akteurs und ausgeführter Aktion; Mindestaufbewahrung 12 Monate.

Minimierung bei der LLM-Inferenz. An den LLM-Proxy wird ausschließlich die strikt notwendige Teilmenge des Profils übergeben; Gesprächsinhalte werden nicht zum Training der Modelle verwendet (DPA mit Anthropic mit vertraglicher No-Training-Klausel).

Pseudonymisierung und Anonymisierung. Gesalzene IP-Hashes; Anwendungsprotokolle ohne Gesprächsinhalt; 30 Tage Protokollaufbewahrung und 90 Tage Aufbewahrung im Fehlermonitor.

Meldung von Verletzungen. Dokumentiertes Verfahren mit Fristen und Verantwortlichen; Mitteilung an den Verantwortlichen innerhalb von 48 Stunden ab Kenntnis.

Kontinuität und Sicherungen. Tägliche automatische Datenbanksicherungen mit 7- bis 30-tägiger Aufbewahrung je nach Plan; periodische Wiederherstellungstests.

Schulung und Vertraulichkeit. Personal des Auftragsverarbeiters durch schriftliche Vertraulichkeitserklärung gebunden; jährliche Schulung in Datenschutz und Informationssicherheit.

Überprüfung. Jährliche Überprüfung der Maßnahmen sowie immer dann, wenn eine neue Schicht, ein neues Modell oder eine wesentliche Änderung der Rechtsgrundlage eingeführt wird.

ANHANG III — GENEHMIGTE UNTER-AUFTRAGSVERARBEITER

Liste der zum Unterschriftsdatum genehmigten Unter-Auftragsverarbeiter. Die aktuelle Fassung wird unter https://afini.ai/de/legal/dpia und in der Datenschutzerklärung gepflegt.

Unter-Auftragsverarbeiter	Dienst	Standort	Garantien
Stripe Payments Europe Ltd.	Zahlungsabwicklung und Rechnungsstellung	Irland (EU)	Auftragsverarbeiter in der EU; PCI-DSS L1; der Auftragsverarbeiter speichert kein PAN.
Anthropic, PBC	LLM-Inferenz (Claude)	Vereinigte Staaten	EU-SCC 2021/914 + vertragliche No-Training-Klausel.
Resend Inc.	Transaktions-E-Mail	Vereinigte Staaten / EU	EU-SCC 2021/914.
Holded Technologies, S.L.	Spanische Rechnungsstellung TicketBAI/BATUZ	Spanien (EU)	Auftragsverarbeiter in der EU.
Railway Corp.	Hosting und PostgreSQL-Datenbank	EU (eu-west)	Verarbeitung in der europäischen Region.
Cloudflare, Inc.	CDN, WAF und DNS	EU (europäisches Netz)	EU-SCC 2021/914 sofern anwendbar.
Functional Software, Inc. (Sentry)	Fehlerüberwachung	EU (Region Frankfurt)	Europäische Verarbeitung.

UNTERSCHRIFTEN

Die Parteien unterzeichnen diesen Vertrag als Zeichen ihrer Zustimmung. Eine qualifizierte oder fortgeschrittene elektronische Signatur mit Zeitstempel gilt gemäß Verordnung (EU) 910/2014 (eIDAS) und dem spanischen Gesetz 6/2020 als der handschriftlichen Signatur gleichwertig.

Für den Verantwortlichen

Firma: _____

USt-IdNr. / Steuernummer: _____

Adresse: _____

Kontakt-E-Mail: _____

Name und Funktion: _____

Datum: _____

Unterschrift: _____

Für den Auftragsverarbeiter — BILBAO AI, S.L.

Firma: BILBAO AI, S.L.

USt-IdNr. / Steuernummer: B-13759758

Adresse: Calle Diputación 8, 4ª pta., dpto. 5 — 48008 Bilbao (Spain)

Kontakt-E-Mail: privacidad@afini.ai

Name und Funktion: _____

Datum: _____

Unterschrift: _____