ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI DA PARTE DEL RESPONSABILE

Ai sensi dell'articolo 28 del regolamento (UE) 2016/679 (GDPR) e dell'articolo 33 della legge organica spagnola 3/2018, del 5 dicembre, sulla protezione dei dati personali e la garanzia dei diritti digitali (LOPDGDD).

TRA

Da una parte, il Cliente identificato nella sezione firma del presente documento, in qualità di Titolare del trattamento (di seguito, il «Titolare»).

E dall'altra parte, BILBAO AI, S.L., codice fiscale spagnolo B-13759758, con sede legale in Calle Diputación 8, 4° piano, ufficio 5, 48008 Bilbao (Spagna), iscritta al Registro delle Imprese di Biscaglia, in qualità di Responsabile del trattamento (di seguito, il «Responsabile» o «Afini.ai»). E-mail per le questioni di privacy: privacidad@afini.ai.

PREMESSE

I. Il Titolare ha contratto o intende contrattare i servizi della piattaforma Afini.ai (compresi, ove applicabile, i prodotti test.afini.ai e/o afini.ai) per il trattamento di dati personali propri o di terzi posti sotto la sua responsabilità.

II. Tale trattamento implica che il Responsabile acceda a dati personali per conto del Titolare, attivando il regime dell'articolo 28 GDPR.

III. Le parti intendono documentare con il presente Accordo le garanzie richieste dalla normativa applicabile.

CLAUSOLE

1. Oggetto

Il presente Accordo regola le condizioni alle quali il Responsabile tratterà dati personali per conto del Titolare in conseguenza della prestazione dei servizi contrattati (di seguito, i «Servizi»). Costituisce parte integrante del contratto principale tra le parti e prevale su di esso in materia di protezione dei dati.

2. Definizioni

I termini «dati personali», «trattamento», «titolare del trattamento», «responsabile del trattamento», «interessato», «violazione dei dati personali», «categorie particolari» e «autorità di controllo» hanno il significato di cui all'articolo 4 GDPR. «Sub-responsabile» indica qualsiasi terzo incaricato dal Responsabile per trattare dati per conto del Titolare.

3. Durata

Il presente Accordo entra in vigore alla data dell'ultima firma e rimane efficace per la durata della prestazione dei Servizi. Gli obblighi che per loro natura debbano sopravvivere alla cessazione (riservatezza, cancellazione, assistenza residuale) sopravvivranno per la durata legalmente richiesta.

4. Natura, finalità e oggetto del trattamento

Il Responsabile tratterà i dati personali descritti nell'Allegato I esclusivamente al fine di prestare i Servizi al Titolare in conformità alle istruzioni documentate del Titolare, comprese l'elaborazione di profili cognitivi, la generazione di rapporti e narrative mediante modelli linguistici, la fatturazione e l'assistenza clienti. Qualsiasi trattamento ulteriore per finalità diverse richiederà istruzione scritta preventiva del Titolare o, in mancanza, una base giuridica autonoma.

5. Tipi di dati personali e categorie di interessati

I tipi di dati e le categorie di interessati sono dettagliati nell'Allegato I. Il trattamento può comprendere categorie particolari ai sensi dell'articolo 9 GDPR (tratti psicologici, valori, stili di attaccamento e altri dati derivati da strumenti psicometrici) qualora il Titolare lo configuri. Il Titolare garantisce l'esistenza di una base giuridica adeguata per il trattamento di tali categorie.

6. Obblighi del Responsabile (art. 28, par. 3 GDPR)

Il Responsabile si impegna a: (a) trattare i dati personali soltanto su istruzioni documentate del Titolare, anche per i trasferimenti internazionali, salvo obbligo di legge contrario, nel qual caso ne darà preventiva comunicazione al Titolare; (b) garantire che le persone autorizzate al trattamento siano vincolate da obbligo di riservatezza o sottoposte a un appropriato obbligo legale di segretezza; (c) adottare tutte le misure richieste ai sensi dell'articolo 32 GDPR; (d) rispettare le condizioni per il ricorso a sub-responsabili di cui alla clausola 7; (e) assistere il Titolare, mediante misure tecniche e organizzative adeguate, per rispondere alle richieste degli interessati di esercizio dei loro diritti; (f) assistere il Titolare nel garantire il rispetto degli obblighi degli articoli da 32 a 36 GDPR, tenendo conto della natura del trattamento e delle informazioni a sua disposizione; (g) a scelta del Titolare, cancellare o restituire tutti i dati personali al termine della prestazione dei Servizi e cancellare le copie esistenti, salvo conservazione richiesta dalla normativa applicabile; (h) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi dell'articolo 28 GDPR e consentire e contribuire ad audit, in conformità alla clausola 12.

7. Sub-responsabili (art. 28, par. 2 GDPR)

Il Titolare autorizza in via generale il Responsabile a ricorrere ai sub-responsabili elencati nell'Allegato III. Il Responsabile stipulerà con ciascun sub-responsabile un contratto scritto che imponga obblighi equivalenti a quelli del presente Accordo. Il Responsabile informerà il Titolare di qualsiasi aggiunta o sostituzione di sub-responsabili con almeno trenta (30) giorni di preavviso tramite la propria Informativa privacy e/o per posta elettronica all'indirizzo di contatto fornito, dando al Titolare l'opportunità di opporsi per motivi ragionevoli. Un'opposizione motivata consentirà al Titolare di risolvere il contratto senza penalità qualora il Responsabile non offra un'alternativa equivalente.

8. Trasferimenti internazionali (Cap. V GDPR)

Qualora il trattamento implichi un trasferimento internazionale al di fuori del SEE (in particolare verso Anthropic, PBC, negli Stati Uniti), il Responsabile farà affidamento su (i) le clausole contrattuali tipo approvate dalla decisione di esecuzione (UE) 2021/914, sottoscritte con il sub-responsabile competente, integrate ove opportuno da (ii) misure supplementari tecniche (cifratura in transito e a riposo, minimizzazione del contenuto trasferito) e organizzative (audit periodici, clausola contrattuale di non addestramento). L'elenco aggiornato dei trasferimenti è riportato nell'Allegato III.

9. Misure tecniche e organizzative (art. 32 GDPR)

Il Responsabile applica le misure tecniche e organizzative descritte nell'Allegato II, che offrono un livello di sicurezza adeguato al rischio. Tali misure sono riviste e aggiornate periodicamente e ogni volta che si introduce una nuova capa, un nuovo modello linguistico o una funzionalità ad alto impatto.

10. Violazioni dei dati personali (art. 33-34 GDPR)

Il Responsabile notificherà al Titolare ogni violazione dei dati personali senza ingiustificato ritardo e in ogni caso entro quarantotto (48) ore dalla conoscenza. La notifica conterrà le informazioni ragionevolmente disponibili e sarà integrata man mano che l'indagine prosegue. Il Responsabile documenta tutte le violazioni, i relativi effetti e le misure correttive adottate.

11. Assistenza al Titolare

Il Responsabile presta al Titolare, mediante misure tecniche e organizzative adeguate, l'assistenza ragionevole per rispondere alle richieste degli interessati di esercizio dei loro diritti (accesso, rettifica, cancellazione, opposizione, limitazione, portabilità e diritto a non essere sottoposti a decisioni automatizzate). Il Responsabile mette a disposizione del Titolare meccanismi di pannello di controllo, esportazione e cancellazione che consentono di soddisfare in autonomia la maggior parte di tali diritti.

12. Audit

Il Responsabile mette a disposizione del Titolare le informazioni necessarie per dimostrare il rispetto dell'articolo 28 GDPR, comprese la sintesi esecutiva della DPIA, la politica di sicurezza e i certificati dei sub-responsabili eventualmente disponibili. Il Titolare può richiedere, con ragionevole preavviso di almeno sessanta (60) giorni e non più di una volta all'anno (salvo incidente grave), un audit documentale o la compilazione di un questionario di tipo SIG-Lite, a proprie spese. Gli audit in loco richiedono il previo accordo delle parti e devono essere condotti durante l'orario lavorativo, senza interferire con l'operatività del Responsabile.

13. Restituzione o cancellazione al termine

Al termine della prestazione dei Servizi, il Responsabile, a scelta del Titolare manifestata per iscritto entro trenta (30) giorni, restituirà o cancellerà i dati personali e cancellerà le copie esistenti, salvo obbligo legale di conservazione. In assenza di istruzione entro tale termine, si applica per impostazione predefinita la cancellazione, che viene registrata nel registro delle attività di trattamento.

14. Responsabilità

Ciascuna parte risponde nei confronti dell'altra dei danni cagionati dall'inadempimento del presente Accordo, conformemente al contratto principale e all'articolo 82 GDPR. Fermo restando la responsabilità solidale nei confronti degli interessati, nel rapporto interno tra le parti il Responsabile risponde solo qualora abbia violato gli obblighi della normativa applicabile o abbia agito al di fuori o in difformità dalle istruzioni del Titolare.

15. Legge applicabile e foro competente

Il presente Accordo è disciplinato dalla legge spagnola e dal diritto dell'Unione europea. Le parti si sottopongono ai Tribunali di Bilbao (Spagna), rinunciando espressamente a qualsiasi altro foro che potesse loro spettare, salva norma imperativa contraria.

ALLEGATO I — DESCRIZIONE DEL TRATTAMENTO

Natura e finalità del trattamento

Prestazione dei Servizi della piattaforma Afini.ai: gestione dell'account e autenticazione, valutazione psicometrica (Big Five e, ove applicabile, capas aggiuntive), elaborazione di profili cognitivi, generazione di rapporti e narrative tramite modelli linguistici, assistenza clienti, fatturazione e manutenzione.

Tipi di dati personali

Dati di identificazione (e-mail, nome e cognome quando forniti), dati di utilizzo del servizio (log applicativi, metriche di utilizzo del proxy LLM, eventi di audit), risposte a questionari psicometrici, conversazioni con l'IA, capas dichiarate del profilo cognitivo, dati di pagamento tokenizzati (gestiti direttamente da Stripe; il Responsabile non memorizza PAN né dati bancari).

Categorie particolari ai sensi dell'art. 9 GDPR

Quando attivate dal Titolare: tratti psicologici (Big Five), stili di umorismo (HSQ), stili di attaccamento (ECR-R), valori personali (AVI), orientamento temporale (ZTPI) e altri dati derivati dalla conversazione cognitivo-estetica.

Categorie di interessati

Utenti finali del Titolare, professionisti invitati dal Titolare sulla piattaforma e, ove applicabile, membri del personale del Titolare.

Durata del trattamento

Per la durata della prestazione dei Servizi, oltre ai termini legali di conservazione ove applicabili.

Luoghi del trattamento

Unione Europea (Railway eu-west, Cloudflare, Sentry regione UE) e, per quanto riguarda l'inferenza LLM, Stati Uniti (Anthropic) sotto clausole contrattuali tipo dell'UE.

ALLEGATO II — MISURE TECNICHE E ORGANIZZATIVE

Cifratura. TLS 1.2 o superiore in transito; AES-256 a riposo nella base dati e nei volumi persistenti.

Controllo accessi. Autenticazione rafforzata con magic-link e/o OAuth, doppio fattore (TOTP e WebAuthn) obbligatorio per gli amministratori; principio del minimo privilegio; rotazione periodica delle credenziali e revoca immediata al termine del rapporto.

Segregazione degli ambienti. Separazione logica tra ambienti di sviluppo, staging e produzione; segreti gestiti come variabili d'ambiente in Railway con scope per servizio.

Tracciabilità. Registro di attività amministrativa con hash dell'IP, identità dell'attore e azione eseguita; ritenzione minima 12 mesi.

Minimizzazione nell'inferenza LLM. Iniezione al proxy LLM esclusivamente del sottoinsieme strettamente necessario del profilo; il contenuto delle conversazioni non viene utilizzato per l'addestramento dei modelli (DPA con Anthropic con clausola contrattuale di non addestramento).

Pseudonimizzazione e anonimizzazione. Hash salati degli IP; log applicativi senza contenuto conversazionale; ritenzione 30 giorni nei log e 90 giorni nel monitor errori.

Notifica violazioni. Procedura documentata con tempi e responsabili; comunicazione al Titolare entro 48 ore dalla conoscenza.

Continuità e backup. Backup automatici giornalieri della base dati con ritenzione 7-30 giorni in base al piano; test di ripristino periodici.

Formazione e riservatezza. Personale del Responsabile vincolato da obbligo scritto di riservatezza; formazione annuale in protezione dei dati e sicurezza delle informazioni.

Revisione. Revisione annuale delle misure e ogni volta che si introduce una nuova capa, un nuovo modello o un cambiamento sostanziale della base giuridica.

ALLEGATO III — SUB-RESPONSABILI AUTORIZZATI

Elenco dei sub-responsabili autorizzati alla data della firma. La versione aggiornata è mantenuta su https://afini.ai/it/legal/dpia e nell'Informativa privacy.

Sub-responsabile	Servizio	Localizzazione	Garanzie
Stripe Payments Europe Ltd.	Gateway di pagamento e fatturazione	Irlanda (UE)	Responsabile in UE; PCI-DSS L1; il Responsabile non memorizza il PAN.
Anthropic, PBC	Inferenza LLM (Claude)	Stati Uniti	SCC UE 2021/914 + clausola contrattuale di non addestramento.
Resend Inc.	E-mail transazionale	Stati Uniti / UE	SCC UE 2021/914.
Holded Technologies, S.L.	Fatturazione spagnola TicketBAI/BATUZ	Spagna (UE)	Responsabile in UE.
Railway Corp.	Hosting e database PostgreSQL	UE (eu-west)	Trattamento nella regione europea.
Cloudflare, Inc.	CDN, WAF e DNS	UE (rete europea)	SCC UE 2021/914 ove applicabili.
Functional Software, Inc. (Sentry)	Monitoraggio errori	UE (regione di Francoforte)	Trattamento europeo.

FIRME

Le parti firmano il presente Accordo in segno di consenso. La firma elettronica qualificata o avanzata con marcatura temporale è considerata equivalente a quella autografa ai sensi del regolamento (UE) 910/2014 (eIDAS) e della legge spagnola 6/2020.

Per il Titolare

Ragione sociale: _____

Codice fiscale / P.IVA: _____

Indirizzo: _____

E-mail di contatto: _____

Nome e qualifica: _____

Data: _____

Firma: _____

Per il Responsabile — BILBAO AI, S.L.

Ragione sociale: BILBAO AI, S.L.

Codice fiscale / P.IVA: B-13759758

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

E-mail di contatto: privacidad@afini.ai

Nome e qualifica: _____

Data: _____

Firma: _____