ACCORD DE SOUS-TRAITANCE DES DONNÉES À CARACTÈRE PERSONNEL

Conformément à l'article 28 du règlement (UE) 2016/679 (RGPD) et à l'article 33 de la loi organique espagnole 3/2018 du 5 décembre relative à la protection des données personnelles et à la garantie des droits numériques (LOPDGDD).

ENTRE

D'une part, le Client identifié dans la section signature du présent document, en qualité de Responsable du traitement (ci-après, le «Responsable»).

Et d'autre part, BILBAO AI, S.L., CIF B-13759758, dont le siège social est situé Calle Diputación 8, 4ᵉ étage, bureau 5, 48008 Bilbao (Espagne), inscrite au Registre du commerce de Biscaye, en qualité de Sous-traitant (ci-après, le «Sous-traitant» ou «Afini.ai»). Courriel pour les questions de confidentialité : privacidad@afini.ai.

EXPOSÉ

I. Le Responsable a souscrit ou s'apprête à souscrire les services de la plateforme Afini.ai (incluant, le cas échéant, les produits test.afini.ai et/ou afini.ai) pour le traitement de données personnelles propres ou de tiers placées sous sa responsabilité.

II. Ce traitement implique que le Sous-traitant accède à des données personnelles pour le compte du Responsable, ce qui déclenche le régime de l'article 28 RGPD.

III. Les parties souhaitent documenter par le présent Accord les garanties exigées par la réglementation applicable.

CLAUSES

1. Objet

Le présent Accord régit les conditions dans lesquelles le Sous-traitant traitera des données personnelles pour le compte du Responsable du fait de la fourniture des services contractés (ci-après, les «Services»). Il fait partie intégrante du contrat principal entre les parties et prévaut sur celui-ci en matière de protection des données.

2. Définitions

Les termes «données à caractère personnel», «traitement», «responsable du traitement», «sous-traitant», «personne concernée», «violation de données», «catégories particulières» et «autorité de contrôle» ont le sens défini à l'article 4 RGPD. «Sous-traitant ultérieur» désigne tout tiers engagé par le Sous-traitant pour traiter des données pour le compte du Responsable.

3. Durée

Le présent Accord entre en vigueur à la date de la dernière signature et reste en vigueur tant que les Services sont fournis. Les obligations qui par leur nature doivent survivre à la résiliation (confidentialité, suppression, assistance résiduelle) survivront pendant la durée légalement requise.

4. Nature, finalité et objet du traitement

Le Sous-traitant traitera les données personnelles décrites à l'Annexe I uniquement aux fins de fourniture des Services au Responsable conformément à ses instructions documentées, y compris l'élaboration de profils cognitifs, la génération de rapports et de récits par des modèles de langage, la facturation et l'assistance client. Tout traitement ultérieur à une finalité distincte nécessitera l'instruction écrite préalable du Responsable ou, à défaut, une base légale indépendante.

5. Types de données et catégories de personnes concernées

Les types de données et les catégories de personnes concernées sont détaillés à l'Annexe I. Le traitement peut inclure des catégories particulières au sens de l'article 9 RGPD (traits psychologiques, valeurs, styles d'attachement et autres données dérivées d'instruments psychométriques) lorsque le Responsable le configure ainsi. Le Responsable garantit l'existence d'une base juridique adéquate pour le traitement de ces catégories.

6. Obligations du Sous-traitant (art. 28, par. 3 RGPD)

Le Sous-traitant s'engage à : (a) traiter les données uniquement sur instructions documentées du Responsable, y compris pour les transferts internationaux, sauf obligation légale contraire, auquel cas il informera le Responsable au préalable ; (b) veiller à ce que les personnes autorisées à traiter les données soient soumises à une obligation de confidentialité ; (c) prendre toutes les mesures requises au titre de l'article 32 RGPD ; (d) respecter les conditions de recours à des sous-traitants ultérieurs énoncées à la clause 7 ; (e) aider le Responsable, par des mesures techniques et organisationnelles appropriées, à répondre aux demandes des personnes concernées d'exercice de leurs droits ; (f) aider le Responsable à garantir le respect des obligations des articles 32 à 36 RGPD, compte tenu de la nature du traitement et des informations à sa disposition ; (g) au choix du Responsable, supprimer ou restituer toutes les données personnelles à la fin de la prestation des Services et supprimer les copies existantes, sauf obligation légale de conservation ; (h) mettre à la disposition du Responsable toutes les informations nécessaires pour démontrer le respect des obligations de l'article 28 RGPD et permettre des audits, conformément à la clause 12.

7. Sous-traitants ultérieurs (art. 28, par. 2 RGPD)

Le Responsable autorise de manière générale le Sous-traitant à recourir aux sous-traitants ultérieurs énumérés à l'Annexe III. Le Sous-traitant conclura avec chaque sous-traitant ultérieur un contrat écrit imposant des obligations équivalentes à celles du présent Accord. Le Sous-traitant informera le Responsable de tout ajout ou remplacement de sous-traitants ultérieurs avec un préavis d'au moins trente (30) jours via sa Politique de confidentialité et/ou par courriel à l'adresse de contact fournie, en donnant au Responsable la possibilité de s'y opposer pour des motifs raisonnables. Une opposition motivée permettra au Responsable de résilier le contrat sans pénalité si le Sous-traitant ne propose pas d'alternative équivalente.

8. Transferts internationaux (Chap. V RGPD)

Lorsque le traitement implique un transfert international hors EEE (notamment vers Anthropic, PBC, aux États-Unis), le Sous-traitant s'appuiera sur (i) les clauses contractuelles types approuvées par la décision d'exécution (UE) 2021/914, signées avec le sous-traitant ultérieur concerné, complétées le cas échéant par (ii) des mesures supplémentaires techniques (chiffrement en transit et au repos, minimisation du

contenu transféré) et organisationnelles (audit périodique, politique contractuelle de non-entraînement). La liste actualisée des transferts figure à l'Annexe III.

9. Mesures techniques et organisationnelles (art. 32 RGPD)

Le Sous-traitant applique les mesures techniques et organisationnelles décrites à l'Annexe II, qui offrent un niveau de sécurité adapté au risque. Ces mesures sont révisées et mises à jour régulièrement et chaque fois qu'une nouvelle couche, un nouveau modèle de langage ou une fonctionnalité à fort impact est introduit.

10. Violations de données (art. 33-34 RGPD)

Le Sous-traitant notifiera au Responsable toute violation de données personnelles sans retard injustifié et, en tout état de cause, dans les quarante-huit (48) heures suivant la prise de connaissance. La notification inclura les informations raisonnablement disponibles et sera complétée à mesure que l'enquête progresse. Le Sous-traitant documentera toutes les violations, leurs effets et les mesures correctives prises.

11. Assistance au Responsable

Le Sous-traitant fournira au Responsable, par des mesures techniques et organisationnelles appropriées, l'assistance raisonnable pour répondre aux demandes des personnes concernées (accès, rectification, suppression, opposition, limitation, portabilité et droit de ne pas faire l'objet de décisions automatisées). Le Sous-traitant met à disposition du Responsable des mécanismes de tableau de bord, d'export et de suppression permettant de satisfaire de manière autonome la plupart de ces droits.

12. Audits

Le Sous-traitant met à la disposition du Responsable les informations nécessaires pour démontrer le respect de l'article 28 RGPD, y compris le résumé exécutif de la DPIA, la politique de sécurité et les certificats de sous-traitants ultérieurs dont il dispose. Le Responsable peut demander, avec un préavis raisonnable d'au moins soixante (60) jours et au maximum une fois par an (sauf incident grave), un audit documentaire ou la réponse à un questionnaire de type SIG-Lite, à ses frais. Les audits sur site nécessitent l'accord préalable des parties et doivent être réalisés pendant les heures de bureau, sans interférer avec les opérations du Sous-traitant.

13. Restitution ou suppression à la fin de la relation

À la fin de la prestation des Services, le Sous-traitant, au choix du Responsable exprimé par écrit dans les trente (30) jours, restitue ou supprime les données personnelles et supprime les copies existantes, sauf obligation légale de conservation. À défaut d'instruction dans ce délai, la suppression s'applique par défaut et est consignée au registre des activités de traitement.

14. Responsabilité

Chaque partie est responsable envers l'autre des dommages causés par la violation du présent Accord, conformément au contrat principal et à l'article 82 RGPD. Sans préjudice de la responsabilité solidaire envers les personnes concernées, dans la relation interne entre les parties, le Sous-traitant n'est responsable que s'il a manqué aux obligations de la réglementation applicable ou s'il a agi en dehors ou contrairement aux instructions du Responsable.

15. Droit applicable et juridiction

Le présent Accord est régi par le droit espagnol et le droit de l'Union européenne. Les parties se soumettent aux tribunaux de Bilbao (Espagne), en renonçant expressément à tout autre for qui pourrait leur être applicable, sauf disposition impérative contraire.

ANNEXE I — DESCRIPTION DU TRAITEMENT

Nature et finalité du traitement

Fourniture des Services de la plateforme Afini.ai : gestion de compte et authentification, évaluation psychométrique (Big Five et, le cas échéant, couches supplémentaires), élaboration de profils cognitifs, génération de rapports et de récits par modèles de langage, support client, facturation et maintenance.

Types de données personnelles

Données d'identification (e-mail, nom et prénom lorsqu'ils sont fournis), données d'utilisation du service (journaux applicatifs, métriques d'utilisation du proxy LLM, événements d'audit), réponses aux questionnaires psychométriques, conversations avec l'IA, couches déclarées du profil cognitif, données de paiement tokenisées (gérées directement par Stripe ; le Sous-traitant ne stocke ni PAN ni données bancaires).

Catégories particulières au sens de l'art. 9 RGPD

Lorsqu'elles sont activées par le Responsable : traits psychologiques (Big Five), styles d'humour (HSQ), styles d'attachement (ECR-R), valeurs personnelles (AVI), orientation temporelle (ZTPI), et autres données dérivées de la conversation cognitive-esthétique.

Catégories de personnes concernées

Utilisateurs finaux du Responsable, professionnels invités par le Responsable sur la plateforme et, le cas échéant, membres du personnel du Responsable.

Durée du traitement

Pendant toute la durée de la prestation des Services, plus les durées légales de conservation lorsqu'elles s'appliquent.

Lieux de traitement

Union européenne (Railway eu-west, Cloudflare, Sentry région UE) et, pour l'inférence LLM, États-Unis (Anthropic) sous clauses contractuelles types de l'UE.

ANNEXE II — MESURES TECHNIQUES ET ORGANISATIONNELLES

Chiffrement. TLS 1.2 ou supérieur en transit ; AES-256 au repos dans la base de données et les volumes persistants.

Contrôle d'accès. Authentification renforcée par lien magique et/ou OAuth, double facteur (TOTP et WebAuthn) obligatoire pour les administrateurs ; principe du moindre privilège ; rotation périodique des identifiants et révocation immédiate à la fin de la relation.

Cloisonnement des environnements. Séparation logique entre les environnements de développement, de pré-production et de production ; secrets gérés en variables d'environnement Railway scoped par service.

Traçabilité. Journal d'activité administratif avec hash d'IP, identité de l'auteur et action effectuée ; rétention minimale 12 mois.

Minimisation à l'inférence LLM. Injection au proxy LLM uniquement du sous-ensemble strictement nécessaire du profil ; le contenu des conversations n'est pas utilisé pour entraîner des modèles (DPA avec Anthropic incluant une clause contractuelle de non-entraînement).

Pseudonymisation et anonymisation. Hashes salés des IP ; journaux applicatifs sans contenu conversationnel ; rétention 30 jours pour les journaux et 90 jours pour le moniteur d'erreurs.

Notification de violations. Procédure documentée avec délais et responsables ; communication au Responsable en moins de 48 h après prise de connaissance.

Continuité et sauvegardes. Sauvegardes quotidiennes automatiques de la base de données avec rétention de 7 à 30 jours selon le plan ; tests de restauration périodiques.

Formation et confidentialité. Personnel du Sous-traitant soumis à une obligation écrite de confidentialité ; formation annuelle en protection des données et sécurité de l'information.

Révision. Révision annuelle des mesures et chaque fois qu'une nouvelle couche, un nouveau modèle ou un changement substantiel de base juridique est introduit.

ANNEXE III — SOUS-TRAITANTS ULTÉRIEURS AUTORISÉS

Liste des sous-traitants ultérieurs autorisés à la date de signature. La version actualisée est tenue à jour sur https://afini.ai/fr/legal/dpia et dans la Politique de confidentialité.

Sous-traitant ultérieur	Service	Localisation	Garanties
Stripe Payments Europe Ltd.	Passerelle de paiement et facturation	Irlande (UE)	Sous-traitant établi dans l'UE ; PCI-DSS L1 ; le Sous-traitant ne stocke pas le PAN.
Anthropic, PBC	Inférence LLM (Claude)	États-Unis	CCT UE 2021/914 + clause contractuelle de non-entraînement.
Resend Inc.	Courriel transactionnel	États-Unis / UE	CCT UE 2021/914.
Holded Technologies, S.L.	Facturation espagnole TicketBAI/BATUZ	Espagne (UE)	Sous-traitant établi dans l'UE.
Railway Corp.	Hébergement et base PostgreSQL	UE (eu-west)	Traitement dans la région européenne.
Cloudflare, Inc.	CDN, WAF et DNS	UE (réseau européen)	CCT UE 2021/914 le cas échéant.
Functional Software, Inc. (Sentry)	Monitoring d'erreurs	UE (région de Francfort)	Traitement européen.

SIGNATURES

Les parties signent le présent Accord en signe d'accord. Une signature électronique qualifiée ou avancée avec horodatage est considérée comme équivalente à la signature manuscrite conformément au règlement (UE) 910/2014 (eIDAS) et à la loi espagnole 6/2020.

Pour le Responsable

Raison sociale : _____

Numéro fiscal : _____

Adresse : _____

Courriel de contact : _____

Nom et fonction : _____

Date : _____

Signature : _____

Pour le Sous-traitant — BILBAO AI, S.L.

Raison sociale : BILBAO AI, S.L.

Numéro fiscal : B-13759758

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

Courriel de contact : privacidad@afini.ai

Nom et fonction : _____

Date : _____

Signature : _____