DATA PROCESSING AGREEMENT

Pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR) and Article 33 of the Spanish Organic Law 3/2018 of 5 December on the Protection of Personal Data and the safeguarding of digital rights (LOPDGDD).

BETWEEN

On the one hand, the Customer identified in the signature section of this document, acting as Data Controller (hereinafter, the "Controller").

And on the other hand, BILBAO AI, S.L., Spanish VAT B-13759758, registered office at Calle Diputación 8, 4th floor, suite 5, 48008 Bilbao (Spain), entered in the Bizkaia Commercial Register, acting as Data Processor (hereinafter, the "Processor" or "Afini.ai"). Email for privacy matters: privacidad@afini.ai.

RECITALS

I. The Controller has engaged or is about to engage the services of the Afini.ai platform (including, as the case may be, the test.afini.ai and/or afini.ai products) to process personal data of its own or of third parties under its responsibility.

II. Such processing entails that the Processor accesses personal data on behalf of the Controller, triggering the regime under Article 28 GDPR.

III. The parties wish to document by means of this Agreement the safeguards required by applicable law.

CLAUSES

1. Subject matter

This Agreement governs the conditions under which the Processor will process personal data on behalf of the Controller as a result of the provision of the contracted services (hereinafter, the "Services"). It forms an integral part of the main contract between the parties and prevails over it as regards data protection.

2. Definitions

The terms "personal data", "processing", "controller", "processor", "data subject", "personal data breach", "special categories" and "supervisory authority" have the meaning set out in Article 4 GDPR. "Sub-processor" means any third party engaged by the Processor to process personal data on behalf of the Controller.

3. Duration

This Agreement enters into force on the date of the last signature and remains in force for as long as the Services are provided. Obligations that by their nature must survive termination (confidentiality, deletion, residual assistance) shall survive for the legally required period.

4. Nature, purpose and subject matter of the processing

The Processor will process the personal data described in Annex I solely for the purpose of providing the Services to the Controller in accordance with its documented instructions, including the building of

cognitive profiles, the generation of reports and narratives by means of language models, billing and customer support. Any further processing for a different purpose shall require the Controller's prior written instruction or, failing that, an independent legal basis.

5. Types of personal data and categories of data subjects

The types of data and categories of data subjects are detailed in Annex I. Processing may include special categories under Article 9 GDPR (psychological traits, values, attachment styles and other data derived from psychometric instruments) where the Controller so configures. The Controller warrants that an adequate legal basis exists for the processing of such categories.

6. Obligations of the Processor (Art. 28(3) GDPR)

The Processor undertakes to: (a) process personal data only on documented instructions from the Controller, including with regard to international transfers, unless required to do so by Union or Member State law to which it is subject, in which case it shall inform the Controller beforehand; (b) ensure that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (c) take all measures required pursuant to Article 32 GDPR; (d) respect the conditions for engaging sub-processors set out in clause 7; (e) assist the Controller, by appropriate technical and organisational measures, in fulfilling its obligation to respond to requests for the exercise of data subject rights; (f) assist the Controller in ensuring compliance with the obligations under Articles 32 to 36 GDPR, taking into account the nature of the processing and the information available to the Processor; (g) at the choice of the Controller, delete or return all personal data after the end of the provision of the Services and delete existing copies, unless retention is required by applicable law; (h) make available to the Controller all information necessary to demonstrate compliance with the obligations of Article 28 GDPR and allow for and contribute to audits, in accordance with clause 12.

7. Sub-processors (Art. 28(2) GDPR)

The Controller grants the Processor general authorisation to engage the sub-processors listed in Annex III. The Processor shall enter into a written contract with each sub-processor imposing obligations equivalent to those of this Agreement. The Processor shall inform the Controller of any addition or replacement of sub-processors at least thirty (30) days in advance through its Privacy Policy and/or by email to the contact address provided, giving the Controller the opportunity to object on reasonable grounds. A reasoned objection shall entitle the Controller to terminate the contract without penalty if the Processor cannot offer an equivalent alternative.

8. International transfers (Chapter V GDPR)

Where processing involves an international transfer outside the EEA (in particular, to Anthropic, PBC, in the United States), the Processor shall rely on (i) the standard contractual clauses approved by Implementing Decision (EU) 2021/914, signed with the relevant sub-processor, supplemented where appropriate by (ii) supplementary technical measures (encryption in transit and at rest, minimisation of the content transferred) and organisational measures (periodic audit, contractual no-training policy). The current list of transfers is set out in Annex III.

9. Technical and organisational measures (Art. 32 GDPR)

The Processor shall apply the technical and organisational measures described in Annex II, which provide a level of security appropriate to the risk. Such measures shall be reviewed and updated periodically and whenever a new layer, a new language model or a high-impact feature is introduced.

10. Personal data breaches (Art. 33-34 GDPR)

The Processor shall notify the Controller of any personal data breach without undue delay and, in any event, within forty-eight (48) hours of becoming aware of it. The notification shall include the information reasonably available and shall be supplemented as the investigation progresses. The Processor shall document all breaches, their effects and the corrective measures taken.

11. Assistance to the Controller

The Processor shall assist the Controller, by appropriate technical and organisational measures, in responding to requests from data subjects to exercise their rights (access, rectification, erasure, objection, restriction, portability and the right not to be subject to automated decisions). The Processor shall make available to the Controller dashboard, export and deletion mechanisms enabling the autonomous fulfilment of most such rights.

12. Audits

The Processor shall make available to the Controller the information necessary to demonstrate compliance with Article 28 GDPR, including the executive summary of the DPIA, the security policy and the certificates of sub-processors that it holds. The Controller may request, with reasonable prior notice of at least sixty (60) days and no more than once a year (save for serious incidents), a documentary audit, or the completion of a SIG-Lite-type questionnaire, at its own cost. On-site audits shall require the prior agreement of the parties and shall be conducted during business hours, without interfering with the Processor's operations.

13. Return or deletion at the end of the relationship

Upon termination of the Services, the Processor shall, at the Controller's choice expressed in writing within thirty (30) days, return or delete personal data and delete existing copies, save for legal retention obligations. Failing instruction within that period, deletion shall apply by default and shall be recorded in the records of processing activities.

14. Liability

Each party shall be liable to the other for damages caused by breach of this Agreement, in accordance with the main contract and Article 82 GDPR. Without prejudice to joint and several liability vis-à-vis data subjects, in the internal relationship between the parties the Processor shall be liable only where it has failed to comply with the obligations of applicable law or has acted outside or contrary to the Controller's instructions.

15. Governing law and jurisdiction

This Agreement shall be governed by Spanish law and Union law. The parties submit to the courts of Bilbao (Spain), expressly waiving any other forum that might apply, except where mandatory rules dictate otherwise.

ANNEX I — DESCRIPTION OF THE PROCESSING

Nature and purpose of the processing

Provision of the Afini.ai platform Services: account management and authentication, psychometric assessment (Big Five and, where applicable, additional layers), construction of cognitive profiles, generation of reports and narratives by means of language models, customer support, billing and maintenance.

Types of personal data

Identification data (email, full name where provided), service usage data (application logs, LLM proxy usage metrics, audit events), responses to psychometric questionnaires, conversations with the AI, declared layers of the cognitive profile, tokenised payment data (handled directly by Stripe; the Processor never stores PAN or banking data).

Special categories under Art. 9 GDPR

Where activated by the Controller: psychological traits (Big Five), humour styles (HSQ), attachment styles (ECR-R), personal values (AVI), time orientation (ZTPI), and other data derived from the cognitive-aesthetic conversation.

Categories of data subjects

End users of the Controller, professionals invited to the platform by the Controller and, where applicable, members of the Controller's staff.

Duration of the processing

For as long as the Services are provided, plus legal retention periods where applicable.

Places of processing

European Union (Railway eu-west, Cloudflare, Sentry EU region) and, with regard to LLM inference, the United States (Anthropic) under EU standard contractual clauses.

ANNEX II — TECHNICAL AND ORGANISATIONAL MEASURES

Encryption. TLS 1.2 or higher in transit; AES-256 at rest in the database and persistent volumes.

Access control. Strong authentication via magic-link and/or OAuth, mandatory multi-factor (TOTP and WebAuthn) for administrators; least-privilege principle; periodic credential rotation and immediate revocation upon termination.

Environment segregation. Logical separation between development, staging and production environments; secrets managed as environment variables in Railway scoped per service.

Traceability. Administrative activity log with hashed IP, actor identity and action performed; minimum 12-month retention.

LLM inference minimisation. Only the strictly necessary subset of the profile is injected into the LLM proxy; conversation content is not used to train models (DPA with Anthropic includes a contractual no-training clause).

Pseudonymisation and anonymisation. Salted IP hashes; application logs without conversation content; 30-day log retention and 90-day error-monitor retention.

Breach notification. Documented procedure with deadlines and owners; notification to the Controller within 48 hours of awareness.

Continuity and backups. Automatic daily database backups with 7- to 30-day retention depending on plan; periodic restoration tests.

Training and confidentiality. Processor staff bound by written confidentiality duty; annual training in data protection and information security.

Review. Annual review of the measures and whenever a new layer, a new model or a substantive change in the legal basis is introduced.

ANNEX III — AUTHORISED SUB-PROCESSORS

List of sub-processors authorised as of the signature date. The current version is maintained at https://afini.ai/en/legal/dpia and in the Privacy Policy.

Sub-processor	Service	Location	Safeguards
Stripe Payments Europe Ltd.	Payment gateway and billing	Ireland (EU)	EU-based processor; PCI-DSS L1; the Processor does not store PAN.
Anthropic, PBC	LLM inference (Claude)	United States	EU SCCs 2021/914 + contractual no-training clause.
Resend Inc.	Transactional email	United States / EU	EU SCCs 2021/914.
Holded Technologies, S.L.	Spanish e-invoicing TicketBAI/BATUZ	Spain (EU)	EU-based processor.
Railway Corp.	Hosting and PostgreSQL database	EU (eu-west)	Processing in the European region.
Cloudflare, Inc.	CDN, WAF and DNS	EU (European network)	EU SCCs 2021/914 where applicable.
Functional Software, Inc. (Sentry)	Error monitoring	EU (Frankfurt region)	European processing.

SIGNATURES

The parties sign this Agreement as evidence of their consent. Qualified or advanced electronic signatures with a time stamp shall be deemed equivalent to handwritten signatures pursuant to Regulation (EU) 910/2014 (eIDAS) and Spanish Law 6/2020.

For the Controller

Company name: _____

VAT / Tax ID: _____

Address: _____

Contact email: _____

Name and title: _____

Date: _____

Signature: _____

For the Processor — BILBAO AI, S.L.

Company name: BILBAO AI, S.L.

VAT / Tax ID: B-13759758

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

Contact email: privacidad@afini.ai

Name and title: _____

Date: _____

Signature: _____