ACUERDO DE ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

Conforme al artículo 28 del Reglamento (UE) 2016/679 (RGPD) y al artículo 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

REUNIDOS

De una parte, el Cliente identificado en la sección de firma de este documento, en su condición de Responsable del Tratamiento (en adelante, el «Responsable»).

Y de otra parte, BILBAO AI, S.L., con CIF B-13759758, domicilio social en Calle Diputación 8, planta 4.ª, departamento 5, 48008 Bilbao (España), inscrita en el Registro Mercantil de Bizkaia, en su condición de Encargado del Tratamiento (en adelante, el «Encargado» o «Afini.ai»). Email para asuntos de privacidad: privacidad@afini.ai.

EXPONEN

I. Que el Responsable ha contratado o se dispone a contratar los servicios de la plataforma Afini.ai (incluyendo, según el caso, los productos test.afini.ai y/o afini.ai) para el tratamiento de datos personales propios o de terceros bajo su responsabilidad.

II. Que dicho tratamiento implica que el Encargado acceda a datos personales por cuenta del Responsable, lo que activa el régimen del artículo 28 RGPD.

III. Que ambas partes desean documentar mediante este Acuerdo las garantías exigidas por la normativa aplicable.

CLÁUSULAS

1. Objeto

El presente Acuerdo regula las condiciones bajo las cuales el Encargado tratará datos personales por cuenta del Responsable como consecuencia de la prestación de los servicios contratados (en adelante, los «Servicios»). Forma parte integrante del contrato principal entre las partes y prevalece sobre éste en lo relativo a la protección de datos.

2. Definiciones

Los términos «datos personales», «tratamiento», «responsable», «encargado», «interesado», «violación de la seguridad», «categorías especiales» y «autoridad de control» tienen el significado del artículo 4 RGPD. «Subencargado» significa cualquier tercero contratado por el Encargado para tratar datos personales por cuenta del Responsable.

3. Duración

Este Acuerdo entra en vigor en la fecha de la última firma y permanecerá vigente mientras dure la prestación de los Servicios. Las obligaciones que por su naturaleza deban subsistir tras la extinción (confidencialidad, supresión, asistencia residual) sobrevivirán durante el plazo legalmente exigible.

4. Naturaleza, finalidad y objeto del tratamiento

El Encargado tratará los datos personales descritos en el Anexo I exclusivamente con la finalidad de prestar los Servicios al Responsable conforme a sus instrucciones documentadas, incluida la elaboración de perfiles cognitivos, la generación de informes y narrativas mediante modelos de lenguaje, la facturación y la atención al cliente. Cualquier tratamiento ulterior con finalidad distinta requerirá la instrucción previa por escrito del Responsable o, en su defecto, base legal independiente.

5. Tipos de datos personales y categorías de interesados

Los tipos de datos y categorías de interesados se detallan en el Anexo I. El tratamiento puede incluir categorías especiales del artículo 9 RGPD (rasgos psicológicos, valores, estilos de apego y otros datos derivados de instrumentos psicométricos) cuando el Responsable así lo configure. El Responsable garantiza la existencia de una base jurídica adecuada para el tratamiento de tales categorías.

6. Obligaciones del Encargado (art. 28.3 RGPD)

El Encargado se obliga a: (a) tratar los datos únicamente siguiendo instrucciones documentadas del Responsable, incluso para transferencias internacionales, salvo obligación legal contraria, en cuyo caso lo notificará previamente; (b) garantizar que las personas autorizadas para tratar datos se hayan comprometido a respetar la confidencialidad o estén sujetas a la obligación legal de secreto; (c) adoptar todas las medidas necesarias en virtud del artículo 32 RGPD; (d) respetar las condiciones para recurrir a subencargados conforme a la cláusula 7; (e) asistir al Responsable, mediante medidas técnicas y organizativas apropiadas, para responder a las solicitudes de ejercicio de derechos por parte de los interesados; (f) ayudar al Responsable a garantizar el cumplimiento de los artículos 32 a 36 RGPD, teniendo en cuenta la naturaleza del tratamiento y la información a su disposición; (g) a elección del Responsable, suprimir o devolver todos los datos personales una vez finalizada la prestación de los Servicios y suprimir las copias existentes, salvo que se requiera la conservación por la legislación aplicable; (h) poner a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones del artículo 28 RGPD, así como permitir y contribuir a auditorías conforme a la cláusula 12.

7. Subencargados (art. 28.2 RGPD)

El Responsable autoriza con carácter general al Encargado a recurrir a los subencargados detallados en el Anexo III. El Encargado celebrará con cada subencargado un contrato escrito que imponga obligaciones equivalentes a las del presente Acuerdo. El Encargado informará al Responsable de cualquier alta o sustitución de subencargados con al menos treinta (30) días de antelación a través de su Política de Privacidad y/o por correo electrónico al email de contacto facilitado, dando ocasión al Responsable a oponerse motivadamente. La oposición razonada permitirá al Responsable resolver el contrato sin penalización si el Encargado no ofreciera una alternativa equivalente.

8. Transferencias internacionales (Cap. V RGPD)

Cuando el tratamiento implique una transferencia internacional fuera del EEE (en particular, a Anthropic, PBC, en EE. UU.), el Encargado se basará en (i) las cláusulas contractuales tipo aprobadas por la Decisión de Ejecución (UE) 2021/914, suscritas con el subencargado correspondiente, complementadas, en su caso, con (ii) medidas suplementarias técnicas (cifrado en tránsito y en reposo, minimización del contenido transferido) y organizativas (auditoría periódica, política contractual de no entrenamiento). El listado de transferencias actualizado figura en el Anexo III.

9. Medidas técnicas y organizativas (art. 32 RGPD)

El Encargado aplicará las medidas técnicas y organizativas descritas en el Anexo II, que ofrecen un nivel de seguridad adecuado al riesgo. Dichas medidas se revisarán y actualizarán periódicamente y siempre que se introduzca una capa nueva, un modelo de lenguaje nuevo o una funcionalidad de alto impacto.

10. Violaciones de la seguridad de los datos (art. 33-34 RGPD)

El Encargado notificará al Responsable cualquier violación de la seguridad de los datos personales sin dilación indebida y, en cualquier caso, dentro de las cuarenta y ocho (48) horas siguientes a tener constancia de la misma. La notificación incluirá la información razonablemente disponible y se irá completando a medida que avance la investigación. El Encargado documentará todas las violaciones, sus efectos y las medidas correctivas adoptadas.

11. Asistencia al Responsable

El Encargado prestará al Responsable, mediante medidas técnicas y organizativas apropiadas, la asistencia razonable para responder a las solicitudes de los interesados de ejercicio de derechos (acceso, rectificación, supresión, oposición, limitación, portabilidad y a no ser objeto de decisiones automatizadas). El Encargado pondrá a disposición del Responsable los mecanismos de panel de control, exportación y supresión que permitan dar cumplimiento autónomo a la mayoría de tales derechos.

12. Auditorías

El Encargado pondrá a disposición del Responsable la información necesaria para acreditar el cumplimiento del artículo 28 RGPD, incluyendo el resumen ejecutivo de la DPIA, la política de seguridad y los certificados de los subencargados que disponga. El Responsable podrá solicitar, con un preaviso razonable de al menos sesenta (60) días y no más de una vez al año (salvo incidente grave), una auditoría documental, o el envío de un cuestionario tipo SIG-Lite, a su costa. Las auditorías presenciales requerirán acuerdo previo de las partes y deberán realizarse en horario laboral, sin interferir en la operativa del Encargado.

13. Devolución o supresión al término

Una vez finalizada la prestación de los Servicios, el Encargado, a elección del Responsable manifestada por escrito en los treinta (30) días siguientes, devolverá o suprimirá los datos personales y suprimirá las copias existentes, salvo obligación legal de conservación. Transcurrido dicho plazo sin instrucción, se procederá a la supresión por defecto, dejando constancia en el registro de actividades.

14. Responsabilidad

Cada parte responderá frente a la otra de los daños que le cause por incumplimiento de este Acuerdo, conforme a lo previsto en el contrato principal y en el artículo 82 RGPD. Sin perjuicio de la responsabilidad solidaria frente a interesados, en la relación interna entre las partes, el Encargado responderá únicamente cuando haya incumplido las obligaciones de la normativa aplicable o haya actuado al margen o en contra de las instrucciones del Responsable.

15. Legislación aplicable y jurisdicción

Este Acuerdo se rige por la legislación española y por el Derecho de la Unión Europea. Las partes se someten a los Juzgados y Tribunales de Bilbao (España), con renuncia expresa a cualquier otro fuero que pudiera corresponderles, salvo norma imperativa en contrario.

ANEXO I — DESCRIPCIÓN DEL TRATAMIENTO

Naturaleza y finalidad del tratamiento

Prestación de los Servicios de la plataforma Afini.ai: gestión de cuenta y autenticación, evaluación psicométrica (Big Five y, en su caso, capas adicionales), elaboración de perfiles cognitivos, generación de informes y narrativas mediante modelos de lenguaje, atención al cliente, facturación y mantenimiento.

Tipos de datos personales

Datos de identificación (email, nombre y apellidos cuando se faciliten), datos de uso del servicio (logs aplicativos, métricas de uso del proxy LLM, eventos de auditoría), respuestas a cuestionarios psicométricos, conversaciones con la IA, capas declaradas del perfil cognitivo, datos de pago tokenizados (gestionados directamente por Stripe; el Encargado no almacena PAN ni datos bancarios).

Categorías especiales del art. 9 RGPD

Cuando el Responsable así lo active: rasgos psicológicos (Big Five), estilos de humor (HSQ), estilos de apego (ECR-R), valores personales (AVI), orientación temporal (ZTPI), y otros datos derivados de la conversación cognitivo-estética.

Categorías de interesados

Usuarios finales del Responsable, profesionales que el Responsable invite a la plataforma, y, en su caso, miembros del personal del Responsable.

Duración del tratamiento

Mientras dure la prestación de los Servicios, más los plazos legales de conservación cuando sean aplicables.

Lugares de tratamiento

Unión Europea (Railway eu-west, Cloudflare, Sentry región de la UE) y, en lo que respecta a la inferencia LLM, Estados Unidos (Anthropic) bajo cláusulas contractuales tipo de la UE.

ANEXO II — MEDIDAS TÉCNICAS Y ORGANIZATIVAS

Cifrado. TLS 1.2 o superior en tránsito; AES-256 en reposo en la base de datos y en los volúmenes persistentes.

Control de acceso. Autenticación reforzada con magic-link y/o OAuth, doble factor (TOTP y WebAuthn) obligatorio para administradores; principio de mínimo privilegio; rotación periódica de credenciales y revocación inmediata al fin de la relación.

Segregación de entornos. Separación lógica entre entornos de desarrollo, staging y producción; secretos gestionados como variables de entorno en Railway con ámbito por servicio.

Trazabilidad. Registro de actividad administrativa con hash de IP, identidad del actor y acción ejecutada; retención mínima de 12 meses.

Minimización en la inferencia LLM. Inyección al proxy LLM exclusivamente del subconjunto del perfil estrictamente necesario; el contenido de las conversaciones no se utiliza para entrenar modelos (DPA con Anthropic con cláusula contractual de no entrenamiento).

Pseudonimización y anonimización. IPs almacenadas con hash salado; logs aplicativos sin contenido conversacional; retención de 30 días en logs y de 90 días en el monitor de errores.

Notificación de violaciones. Procedimiento documentado con plazos y responsables; comunicación al Responsable en menos de 48 h desde el conocimiento.

Continuidad y copias de seguridad. Copias diarias automáticas de la base de datos con retención de 7 a 30 días según plan; pruebas periódicas de restauración.

Formación y confidencialidad. Personal del Encargado sujeto a deber de confidencialidad escrito; formación anual en protección de datos y seguridad de la información.

Revisión. Revisión anual de las medidas y siempre que se introduzca una capa nueva, un modelo nuevo o un cambio sustantivo en la base jurídica.

ANEXO III — SUBENCARGADOS AUTORIZADOS

Listado de subencargados autorizados a la fecha de firma. La versión actualizada se mantiene en https://afini.ai/es/legal/dpia y en la Política de Privacidad.

Subencargado	Servicio	Localización	Garantías
Stripe Payments Europe Ltd.	Pasarela de pago y facturación	Irlanda (UE)	Encargado en la UE; PCI-DSS L1; el Encargado no almacena PAN.
Anthropic, PBC	Inferencia LLM (Claude)	Estados Unidos	SCCs UE 2021/914 + cláusula contractual de no entrenamiento.
Resend Inc.	Email transaccional	Estados Unidos / UE	SCCs UE 2021/914.
Holded Technologies, S.L.	Facturación TicketBAI/BATUZ	España (UE)	Encargado en la UE.
Railway Corp.	Hosting y base de datos PostgreSQL	UE (eu-west)	Procesamiento en la región europea.
Cloudflare, Inc.	CDN, WAF y DNS	UE (red europea)	SCCs UE 2021/914 cuando aplique.
Functional Software, Inc. (Sentry)	Monitorización de errores	UE (región de Frankfurt)	Procesamiento europeo.

FIRMAS

Las partes firman este Acuerdo en señal de conformidad. La firma digital cualificada o avanzada con sello de tiempo se considera equivalente a la manuscrita conforme al Reglamento (UE) 910/2014 (eIDAS) y la Ley 6/2020.

Por el Responsable

Razón social: _____

CIF / NIF: _____

Domicilio: _____

Email de contacto: _____

Nombre y cargo: _____

Fecha: _____

Firma: _____

Por el Encargado — BILBAO AI, S.L.

Razón social: BILBAO AI, S.L.

CIF / NIF: B-13759758

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

Email de contacto: privacidad@afini.ai

Nombre y cargo: _____

Fecha: _____

Firma: _____