ACORDO DE SUBCONTRATANTE DO TRATAMENTO DE DADOS PESSOAIS

Conforme o artigo 28.º do Regulamento (UE) 2016/679 (RGPD) e o artigo 33.º da Lei Orgânica espanhola 3/2018, de 5 de dezembro, sobre proteção de dados pessoais e garantia dos direitos digitais (LOPDGDD).

ENTRE

De um lado, o Cliente identificado na seção de assinatura deste documento, na qualidade de Responsável pelo Tratamento (doravante, o «Responsável»).

E do outro lado, BILBAO AI, S.L., NIF espanhol B-13759758, com sede em Calle Diputación 8, 4.º andar, gabinete 5, 48008 Bilbao (Espanha), inscrita no Registo Mercantil de Biscaia, na qualidade de Subcontratante (doravante, o «Subcontratante» ou «Afini.ai»). E-mail para questões de privacidade: privacidad@afini.ai.

CONSIDERANDOS

I. O Responsável contratou ou está prestes a contratar os serviços da plataforma Afini.ai (incluindo, conforme o caso, os produtos test.afini.ai e/ou afini.ai) para o tratamento de dados pessoais próprios ou de terceiros sob a sua responsabilidade.

II. Esse tratamento implica que o Subcontratante aceda a dados pessoais por conta do Responsável, ativando o regime do artigo 28.º do RGPD.

III. As partes desejam documentar por meio do presente Acordo as garantias exigidas pela legislação aplicável.

CLÁUSULAS

1. Objeto

O presente Acordo regula as condições em que o Subcontratante tratará dados pessoais por conta do Responsável em consequência da prestação dos serviços contratados (doravante, os «Serviços»). Faz parte integrante do contrato principal entre as partes e prevalece sobre ele em matéria de proteção de dados.

2. Definições

Os termos «dados pessoais», «tratamento», «responsável pelo tratamento», «subcontratante», «titular dos dados», «violação de dados pessoais», «categorias especiais» e «autoridade de controlo» têm o significado definido no artigo 4.º do RGPD. «Subcontratante ulterior» significa qualquer terceiro contratado pelo Subcontratante para tratar dados por conta do Responsável.

3. Duração

O presente Acordo entra em vigor na data da última assinatura e mantém-se em vigor enquanto durarem os Serviços. As obrigações que pela sua natureza devam subsistir após a cessação (confidencialidade, eliminação, assistência residual) sobreviverão pelo prazo legalmente exigido.

4. Natureza, finalidade e objeto do tratamento

O Subcontratante tratará os dados pessoais descritos no Anexo I exclusivamente para a prestação dos Serviços ao Responsável conforme as suas instruções documentadas, incluindo a elaboração de perfis cognitivos, a geração de relatórios e narrativas mediante modelos de linguagem, a faturação e o atendimento ao cliente. Qualquer tratamento ulterior com finalidade distinta exigirá instrução escrita prévia do Responsável ou, na sua ausência, base jurídica autónoma.

5. Tipos de dados pessoais e categorias de titulares

Os tipos de dados e categorias de titulares são detalhados no Anexo I. O tratamento pode incluir categorias especiais ao abrigo do artigo 9.º do RGPD (traços psicológicos, valores, estilos de vínculo e outros dados derivados de instrumentos psicométricos) quando o Responsável o configurar. O Responsável garante a existência de base jurídica adequada para o tratamento de tais categorias.

6. Obrigações do Subcontratante (art. 28.º, n.º 3, RGPD)

O Subcontratante compromete-se a: (a) tratar dados pessoais apenas com base em instruções documentadas do Responsável, incluindo no que respeita a transferências internacionais, salvo obrigação legal contrária, caso em que informará previamente o Responsável; (b) garantir que as pessoas autorizadas a tratar dados se comprometeram à confidencialidade ou estão sujeitas a um adequado dever legal de sigilo; (c) tomar todas as medidas exigidas pelo artigo 32.º do RGPD; (d) respeitar as condições de recurso a subcontratantes ulteriores nos termos da cláusula 7; (e) auxiliar o Responsável, mediante medidas técnicas e organizativas adequadas, a responder a pedidos dos titulares para o exercício dos seus direitos; (f) auxiliar o Responsável a garantir o cumprimento das obrigações dos artigos 32.º a 36.º do RGPD, tendo em conta a natureza do tratamento e as informações ao seu dispor; (g) à escolha do Responsável, eliminar ou devolver todos os dados pessoais após o termo da prestação dos Serviços e eliminar as cópias existentes, salvo obrigação legal de conservação; (h) disponibilizar ao Responsável toda a informação necessária para demonstrar o cumprimento das obrigações do artigo 28.º do RGPD e permitir e contribuir para auditorias, em conformidade com a cláusula 12.

7. Subcontratantes ulteriores (art. 28.º, n.º 2, RGPD)

O Responsável autoriza, com caráter geral, o Subcontratante a recorrer aos subcontratantes ulteriores listados no Anexo III. O Subcontratante celebrará com cada subcontratante ulterior um contrato escrito que imponha obrigações equivalentes às do presente Acordo. O Subcontratante informará o Responsável de qualquer adição ou substituição de subcontratantes ulteriores com pelo menos trinta (30) dias de antecedência através da sua Política de Privacidade e/ou por correio eletrónico ao endereço de contacto fornecido, dando ao Responsável a oportunidade de se opor por motivos razoáveis. Uma oposição fundamentada permitirá ao Responsável rescindir o contrato sem penalização caso o Subcontratante não ofereça uma alternativa equivalente.

8. Transferências internacionais (Cap. V RGPD)

Quando o tratamento implicar uma transferência internacional para fora do EEE (em particular, para a Anthropic, PBC, nos EUA), o Subcontratante apoiar-se-á em (i) cláusulas contratuais-tipo aprovadas pela Decisão de Execução (UE) 2021/914, celebradas com o subcontratante ulterior em causa, complementadas, sempre que adequado, por (ii) medidas suplementares técnicas (cifragem em trânsito e em repouso, minimização do conteúdo transferido) e organizativas (auditoria periódica, cláusula contratual de não treinamento). A lista atualizada das transferências consta no Anexo III.

9. Medidas técnicas e organizativas (art. 32.º RGPD)

O Subcontratante aplica as medidas técnicas e organizativas descritas no Anexo II, que oferecem um nível de segurança adequado ao risco. Tais medidas são revistas e atualizadas periodicamente e sempre que se introduza uma camada nova, um modelo de linguagem novo ou uma funcionalidade de alto impacto.

10. Violações de dados pessoais (art. 33.º-34.º RGPD)

O Subcontratante notificará o Responsável de qualquer violação de dados pessoais sem atraso indevido e, em qualquer caso, no prazo de quarenta e oito (48) horas a contar do conhecimento. A notificação incluirá a informação razoavelmente disponível e será complementada à medida que a investigação avance. O Subcontratante documenta todas as violações, os respetivos efeitos e as medidas corretivas adotadas.

11. Assistência ao Responsável

O Subcontratante presta ao Responsável, mediante medidas técnicas e organizativas adequadas, a assistência razoável para responder a pedidos dos titulares de exercício dos seus direitos (acesso, retificação, eliminação, oposição, limitação, portabilidade e direito a não ficarem sujeitos a decisões automatizadas). O Subcontratante disponibiliza ao Responsável mecanismos de painel, exportação e eliminação que permitem cumprir autonomamente a maior parte de tais direitos.

12. Auditorias

O Subcontratante disponibiliza ao Responsável a informação necessária para demonstrar o cumprimento do artigo 28.º do RGPD, incluindo o resumo executivo da DPIA, a política de segurança e os certificados dos subcontratantes ulteriores que tenha. O Responsável pode solicitar, com aviso prévio razoável de pelo menos sessenta (60) dias e não mais do que uma vez por ano (salvo incidente grave), uma auditoria documental ou o preenchimento de um questionário do tipo SIG-Lite, a expensas suas. As auditorias presenciais exigem acordo prévio das partes e devem ser realizadas em horário laboral, sem interferir na operação do Subcontratante.

13. Devolução ou eliminação ao termo

Após o termo da prestação dos Serviços, o Subcontratante, à escolha do Responsável manifestada por escrito nos trinta (30) dias seguintes, devolverá ou eliminará os dados pessoais e eliminará as cópias existentes, salvo obrigação legal de conservação. Decorrido esse prazo sem instrução, será aplicada por padrão a eliminação, ficando registada no registo de atividades de tratamento.

14. Responsabilidade

Cada parte responde perante a outra pelos danos que lhe cause por incumprimento do presente Acordo, conforme previsto no contrato principal e no artigo 82.º do RGPD. Sem prejuízo da responsabilidade solidária perante os titulares, na relação interna entre as partes, o Subcontratante apenas responde quando tenha violado as obrigações da regulamentação aplicável ou tenha atuado fora ou em contrário às instruções do Responsável.

15. Lei aplicável e jurisdição

O presente Acordo rege-se pela lei espanhola e pelo Direito da União Europeia. As partes submetem-se aos Tribunais de Bilbao (Espanha), renunciando expressamente a qualquer outro foro que lhes pudesse caber, salvo norma imperativa em contrário.

ANEXO I — DESCRIÇÃO DO TRATAMENTO

Natureza e finalidade do tratamento

Prestação dos Serviços da plataforma Afini.ai: gestão de conta e autenticação, avaliação psicométrica (Big Five e, conforme o caso, camadas adicionais), elaboração de perfis cognitivos, geração de relatórios e narrativas mediante modelos de linguagem, atendimento ao cliente, faturação e manutenção.

Tipos de dados pessoais

Dados de identificação (e-mail, nome e apelidos quando fornecidos), dados de utilização do serviço (logs aplicacionais, métricas de uso do proxy LLM, eventos de auditoria), respostas a questionários psicométricos, conversas com a IA, camadas declaradas do perfil cognitivo, dados de pagamento tokenizados (geridos diretamente por Stripe; o Subcontratante não armazena PAN nem dados bancários).

Categorias especiais ao abrigo do art. 9.º do RGPD

Quando ativadas pelo Responsável: traços psicológicos (Big Five), estilos de humor (HSQ), estilos de vínculo (ECR-R), valores pessoais (AVI), orientação temporal (ZTPI) e outros dados derivados da conversa cognitivo-estética.

Categorias de titulares

Utilizadores finais do Responsável, profissionais convidados pelo Responsável para a plataforma e, conforme o caso, membros do pessoal do Responsável.

Duração do tratamento

Enquanto durar a prestação dos Serviços, acrescidos dos prazos legais de conservação quando aplicáveis.

Locais de tratamento

União Europeia (Railway eu-west, Cloudflare, Sentry região UE) e, no que respeita à inferência LLM, Estados Unidos (Anthropic) sob cláusulas contratuais-tipo da UE.

ANEXO II — MEDIDAS TÉCNICAS E ORGANIZATIVAS

Cifragem. TLS 1.2 ou superior em trânsito; AES-256 em repouso na base de dados e nos volumes persistentes.

Controlo de acesso. Autenticação reforçada por magic-link e/ou OAuth, duplo fator (TOTP e WebAuthn) obrigatório para administradores; princípio do mínimo privilégio; rotação periódica de credenciais e revogação imediata ao termo da relação.

Segregação de ambientes. Separação lógica entre ambientes de desenvolvimento, staging e produção; segredos geridos como variáveis de ambiente em Railway com escopo por serviço.

Rastreabilidade. Registo de atividade administrativa com hash de IP, identidade do ator e ação executada; retenção mínima 12 meses.

Minimização na inferência LLM. Injeção no proxy LLM exclusivamente do subconjunto estritamente necessário do perfil; o conteúdo das conversas não é utilizado para treinar modelos (DPA com Anthropic com cláusula contratual de não treinamento).

Pseudonimização e anonimização. Hashes salgados de IP; logs aplicacionais sem conteúdo conversacional; retenção 30 dias nos logs e 90 dias no monitor de erros.

Notificação de violações. Procedimento documentado com prazos e responsáveis; comunicação ao Responsável em menos de 48 h após o conhecimento.

Continuidade e cópias de segurança. Cópias diárias automáticas da base de dados com retenção de 7 a 30 dias conforme o plano; testes periódicos de restauro.

Formação e confidencialidade. Pessoal do Subcontratante sujeito a dever escrito de confidencialidade; formação anual em proteção de dados e segurança da informação.

Revisão. Revisão anual das medidas e sempre que se introduza uma camada nova, um modelo novo ou uma alteração substantiva da base jurídica.

ANEXO III — SUBCONTRATANTES ULTERIORES AUTORIZADOS

Lista dos subcontratantes ulteriores autorizados à data da assinatura. A versão atualizada é mantida em https://afini.ai/pt/legal/dpia e na Política de Privacidade.

Subcontratante ulterior	Serviço	Localização	Garantias
Stripe Payments Europe Ltd.	Gateway de pagamento e faturação	Irlanda (UE)	Subcontratante na UE; PCI-DSS L1; o Subcontratante não armazena PAN.
Anthropic, PBC	Inferência LLM (Claude)	Estados Unidos	CCT UE 2021/914 + cláusula contratual de não treinamento.
Resend Inc.	E-mail transacional	Estados Unidos / UE	CCT UE 2021/914.
Holded Technologies, S.L.	Faturação espanhola TicketBAI/BATUZ	Espanha (UE)	Subcontratante na UE.
Railway Corp.	Hosting e base de dados PostgreSQL	UE (eu-west)	Tratamento na região europeia.
Cloudflare, Inc.	CDN, WAF e DNS	UE (rede europeia)	CCT UE 2021/914 quando aplicáveis.
Functional Software, Inc. (Sentry)	Monitorização de erros	UE (região de Frankfurt)	Tratamento europeu.

ASSINATURAS

As partes assinam o presente Acordo em sinal de conformidade. A assinatura eletrónica qualificada ou avançada com selo temporal é considerada equivalente à manuscrita conforme o Regulamento (UE) 910/2014 (eIDAS) e a Lei espanhola 6/2020.

Pelo Responsável

Razão social: _____

NIF / CNPJ: _____

Morada: _____

E-mail de contacto: _____

Nome e cargo: _____

Data: _____

Assinatura: _____

Pelo Subcontratante — BILBAO AI, S.L.

Razão social: BILBAO AI, S.L.

NIF / CNPJ: B-13759758

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

E-mail de contacto: privacidad@afini.ai

Nome e cargo: _____

Data: _____

Assinatura: _____