Aidealy Ltd.
Hamidron 1, Herzliya 4654110, Israel
aidealy.ai | legal@aidealy.ai

Aidealy Sub-processor List & Policy

Effective date: 2026-11-03 · Version: 1.6.0 · Last updated: 2026-11-03

Introduction

A **sub-processor** is a third party that we engage to process personal data on our behalf - or, for some categories of data, a service provider that processes personal data for which we are responsible - in order to provide and operate our service. **Aidealy Ltd.** ("Aidealy", "we") engages the third parties listed below.

We organise them into two tiers, because our role differs between them:

- **Tier A - Service sub-processors.** These process customer **work data** (your source code, AI prompts and responses, git author identity and developer-activity metrics). For this data your organisation is the controller and Aidealy is a **processor** acting on your instructions under our **Data Processing Agreement (DPA)**. The vendors in Tier A are the sub-processors authorised in the DPA (Annex III), and "Customer Personal Data" in this section has the meaning given in the DPA.
- **Tier B - Account & business-operations service providers.** These process **account data** (the identity, authentication, security, billing and related information of the people who sign in to Aidealy) and our business-operations data (including data about visitors to our website). For this data Aidealy is the **controller** and these providers act for us; that processing is governed by our **Privacy Policy**, not the DPA.

This list is a transparency commitment. It is also the customer-facing record of the sub-processors authorised under our DPA.

Tier A - Service sub-processors

These third parties process customer **work data**; Aidealy acts as your **processor** under the DPA, and these are the sub-processors listed in DPA Annex III.

Sub-processor	Service / purpose	Processing location(s)
Amazon Web Services, Inc.	Cloud compute and storage, including the Amazon Bedrock AgentCore Code Interpreter (a sandbox in the customer's own region that executes the analysis code the analytics assistant generates over that customer's query results)	EU (eu-west-1) / US (per customer region)
Anthropic, PBC	AI model provider - the AI features of the Service (analysis and scoring of source code, classification of developers' typed messages, and the natural-language analytics assistant). Aidealy routes each AI step to either of its two listed AI model	United States (no EU option; stores API data in the United States)

© 2026 Aidealy Ltd.

Sub-processor	Service / purpose	Processing location(s)
	providers and may change that routing at any time, including as a fallback, without adding a sub-processor; each provider's own retention terms are disclosed in DPA §10. Usage policy: see the AI-provider note below	
OpenAI OpCo, LLC	AI model provider - the AI features of the Service (analysis and scoring of source code, classification of developers' typed messages, and the natural-language analytics assistant). Aidealy routes each AI step to either of its two listed AI model providers and may change that routing at any time, including as a fallback, without adding a sub-processor; each provider's own retention terms are disclosed in DPA §10. Stores the analytics assistant's conversation history server-side where the assistant is routed to it. Usage policy: see the AI-provider note below	EU/US (per project or per request); processing at OpenAI's default endpoint (a United States recipient; OpenAI's EU regional option is supported in Aidealy's software but not switched on)
ArangoDB GmbH	Managed graph database - code graph and stored code/ diff content	EU (eu-west-1) / US (per customer region)
Supabase, Inc.	Managed database and authentication	EU (eu-west-1) / US (per customer region)
Functional Software, Inc. (dba Sentry)	Application error monitoring (incl. masked session replay on errors)	EU / US (per customer region)
Vercel, Inc.	Hosting of the web applications	EU (eu-west-1) / US (per customer region)
LangChain, Inc. (LangSmith)	LLM tracing / observability of the AI features (integration wired but dormant - no data flows until activated)	United States

Notes:

- We operate **both regions today - EU (eu-west-1) and US** - and each customer organisation selects its region at onboarding; a US selection is never silently deployed to the EU. The region-

scoped infrastructure vendors above (AWS, ArangoDB, Supabase, Vercel) process a tenant's work data in that tenant's selected region; Sentry runs in both EU and US, per the customer's region.

- Some providers contract through a regional affiliate. For EEA/EMEA customers, Amazon Web Services is provided by **Amazon Web Services EMEA SARL** (Luxembourg); OpenAI's contracting entity is determined by the customer's location under OpenAI's Services Agreement (**OpenAI OpCo, LLC** for a customer outside the EEA and Switzerland, which is Aidealy's case). ArangoDB is contracted through **ArangoDB GmbH** (Germany).
- LangSmith is listed on a **forward basis**: its tracing integration is wired in our shipped production software but **dormant** - no LangSmith API key is provisioned, so **no customer personal data flows to LangChain today**; we will activate the flow only once LangChain's data-processing terms are executed and on file. LangSmith is **not region-separated**: the wiring uses LangChain's default **United-States** endpoint (no EU data-residency pinning), so tracing data - once activated - is processed in the US under the SCC mechanism in Annex IV of our DPA.
- The **AI-model inference leg is the one exception** to our region-separation model. Whichever of the two listed AI model providers Aidealy routes a step to, the content is processed in the **United States**: **Anthropic** stores API data in the United States and its first-party API has **no EU data-residency option**, so inference geography is not guaranteed for non-US tenants - even for EU-region accounts; **OpenAI** processes at its default endpoint (its EU regional option is supported in our software but not switched on) and, where the analytics assistant is routed to it, stores that assistant's conversation history server-side in the United States. Only the content submitted for an AI step (the source code sent for scoring, the typed messages sent for classification, and the assistant's inputs, together with, for the assistant, the conversation history OpenAI keeps) leaves your region: each provider holds that content under its own retention terms set out in DPA §10 and it is **not used to train any model** by either provider, while your **stored** work data stays in your region. These onward transfers are safeguarded by the **EU Standard Contractual Clauses (Module 3)** in Annex IV of our DPA; each provider's retention terms are set out in DPA §10.
- ***AI-provider roles and routing.** Each AI provider above is authorised as an **AI model provider for all the AI features of the Service**: the analysis and scoring of source code, the classification of developers' typed messages (which labels each message on four points: the part of the system it is about, the kind of work asked for, any quality concern raised, and its apparent tone), and the natural-language analytics assistant. Either provider may perform any of those steps; Aidealy chooses the routing and may change it at any time - including as a fallback when one provider is unavailable - without a change notice, because no new entity receives your data; adding or replacing a provider **entity** triggers the notice-and-objection process below. AI models Aidealy operates on its own infrastructure (including inside its own cloud account, where the model provider has no access to customer content) are Aidealy's own processing, not a sub-processor. (See the AI Addendum §1.6 and DPA §6.2.)
- ***AI-provider usage policies.** Your use of the AI features must comply with the listed AI providers' published usage policies (see the Acceptable Use Policy, Section 3.14). The current policies are published by the providers here: **Anthropic** - Usage Policy, at anthropic.com/legal/aup; **OpenAI** - Usage Policies, at openai.com/policies/usage-policies. The version that applies to particular conduct is the version in effect at the time of that conduct; if a provider moves its policy, the successor page it designates applies.

Tier B - Account & business-operations service providers

These third parties process **account data** and our business-operations data, for which Aidealy is the **controller**; their processing is governed by our **Privacy Policy**. Cross-border transfers for these providers are covered by their own data-processing agreements (which use the EU Standard Contractual Clauses or another GDPR transfer safeguard and, where applicable, the UK Addendum), described in our Privacy Policy rather than in the DPA's Annex IV.

Service provider	Service / purpose	Processing location(s)	Our role
Cloudflare, Inc.	Bot protection (Turnstile) on the sign-in and website contact forms	EU / global (edge)	Controller (Cloudflare = processor)
Mailgun Technologies, Inc. (Sinch)	Sending account and product emails (transactional and authentication messages), delivering website contact-form enquiries to us, and sending us a weekly summary of the organisations that visited our website	EU (for EU customers; website emails use the EU endpoint); US (for US customers)	Controller (Mailgun = processor)
Paddle.com Market Ltd. (UK) / Paddle.com Inc. (US)	Payment processing as Merchant of Record (checkout, tax/VAT, refunds, chargebacks)	UK / EU and US	See note below
Google Cloud EMEA Limited (Google Workspace)	Corporate email and document storage (business correspondence)	Any country where Google or its sub-processors maintain facilities (our Google Workspace plan offers no data-region setting)	Controller (Google = processor)
HubSpot, Inc. and its affiliates	CRM, email and marketing for our website: stores the details submitted through the website contact form, including any opt-in to marketing emails and the page the form was sent from; records, for visitors who accept marketing cookies, the pages they view, linked to their enquiry if they send one, and the organisations that visited our website; and is used for	EU (HubSpot's EU data centre, Germany); may also be processed by HubSpot, Inc. in the United States and by HubSpot affiliates and sub-processors in other countries	Controller (HubSpot = processor)

Service provider	Service / purpose	Processing location(s)	Our role
	marketing to people who opted in		
Nikolai Tschacher, trading as ipapi.is (Berlin, Germany)	Identifying the organisation behind a website visitor's IP address, only for visitors who accept marketing cookies; the IP address is not stored	Germany only (servers operated by Hetzner Online GmbH, Germany)	Controller (ipapi.is = processor)
Plausible Insights OÜ (Plausible Analytics)	Cookieless website analytics (aggregated statistics about how visitors use our website); runs only after a visitor accepts statistics cookies in our consent banner, and does not store IP addresses or set persistent identifiers	EU (stored in Germany; not transferred outside the EU)	Controller (Plausible = processor)
Usercentrics A/S (Cookiebot)	Cookie-consent management for our website: the consent banner and the consent log. The log records each visitor's consent (a consent identifier, the consent state and the policy version consented to, the page URL, the browser user agent, the first half of the IP address, the date and time, and an encrypted key), is processed within the EU/EEA and is deleted after 12 months, after which only aggregated, anonymised statistics remain. The request that loads the banner before any choice is made (IP address, browser user agent,	Consent log: EU (Microsoft Azure, Ireland, with fail-over to Amsterdam, Netherlands). Banner delivery: the content-delivery network of Akamai Technologies, Inc. (a United States company; may handle the request outside Europe)	Controller (Usercentrics = processor)

Service provider	Service / purpose	Processing location(s)	Our role
	page URL and browser language) is served through the content-delivery network of Akamai Technologies, Inc., a United States company, which may handle the request outside Europe and may log connection details, including the visitor's IP address; Cookiebot itself uses that request only to serve the banner and keeps none of it after processing		

Notes:

- ***Paddle's role.*** We use Paddle as our **Merchant of Record**. For payment, tax and fraud-prevention purposes Paddle acts as a **separate, independent controller** of buyer payment data - that is, not solely our service provider - and Paddle's own privacy terms govern that processing. We therefore do not describe Paddle simply as "our processor". Paddle's handling of buyer payment data is described in **Paddle's Privacy Notice** (paddle.com/legal/privacy), and our data-sharing arrangement with Paddle is governed by Paddle's **Data Sharing Addendum** (paddle.com/legal/data-sharing-addendum). For an Israel-based supplier, the contracting Paddle entity is **Paddle.com Market Limited** (the UK-supplier entity Paddle Payments Limited does not apply to us). **On termination, we cancel the customer's active subscriptions and archive its Paddle customer record; Paddle retains the underlying invoice/tax records under its own statutory retention periods as Merchant of Record (it does not provide for deletion of those records).**
- Our Google Workspace contract is with **Google Cloud EMEA Limited** (Dublin, Ireland). Mailgun is the email brand of the **Sinch** group; the specific Sinch contracting entity depends on the customer's region and order form.
- **HubSpot**, **ipapi.is**, **Plausible** and **Cookiebot** serve our marketing website only and never receive customer work data; our **Website Privacy Policy** describes their processing. Cookiebot is operated by **Usercentrics A/S** (Havnegade 39, 1058 Copenhagen, Denmark). Under its data-processing agreement, any transfer of the data it processes for us outside the EU/EEA may take place only where the GDPR's transfer safeguards are met (the agreement names, among others, the Commission's adequacy decisions and the EU Standard Contractual Clauses); its own sub-processors are listed in Annex 2 of that agreement (including Microsoft Ireland Operations Ltd for hosting; Akamai Technologies, Inc., United States, for banner delivery and geolocation).

Changes to our sub-processors (notice and right to object)

We maintain this list as our current record of authorised sub-processors. Before we engage any **new or replacement** sub-processor, **we will notify all active customers by email at least 30 days before that sub-processor begins processing Customer Personal Data.**

Within that period, a customer may **object** to the change on reasonable data-protection grounds. An objection should be in writing and state the specific data-protection grounds it rests on. We will

work with you in good faith to resolve the objection - including, where commercially feasible, by continuing to provide the Service to you without the new sub-processor. If we cannot resolve it, your **sole remedy** is to **terminate the part of the Service that cannot be provided without that sub-processor**, and we will refund any prepaid, unused fees for that part.

A "**new or replacement sub-processor**" means a change of **entity** - adding an entity not on this list, or replacing a listed entity with another. Routing work among entities already on this list (each within its disclosed role), and AI models Aidealy operates on its own infrastructure, are not changes requiring notice (see the AI-provider notes above).

Re-allocation among the listed AI providers. Both AI model providers on this list are authorised for all the AI features of the Service. A change in which listed provider handles a given AI feature - whether Aidealy chooses it, a new model release prompts it, or one provider becomes unavailable and the other takes over - is a re-allocation among sub-processors you have already authorised: it is not a new or replacement sub-processor, opens no objection window and requires no notice under this section. Adding a provider that is not on this list, or replacing a listed one, remains a change of entity announced as described above.

Emergency replacement. If a sub-processor suddenly becomes unavailable, or we must replace it urgently to keep the Service running securely (for example, an abrupt cutoff by an AI provider), we may engage a replacement **before** the 30-day notice period has run. In that case we will notify all active customers **without undue delay**, identifying the replacement, its role, locations, and transfer safeguards; the required data-protection terms are put in place **before** the replacement processes customer personal data; and your **objection right is preserved** - you may object within 30 days of our notice, with the same remedy as above.

This reflects the general written authorisation given in our DPA: under data-protection law a processor operating on a general authorisation must actively inform the controller of any intended addition or replacement of sub-processors and give an opportunity to object.

This channel is stated identically in our **DPA §6.2** (reconciled 2026-06-17 to the same email-to-all-active-customers mechanism), so the two documents match.

International transfers

Aidealy Ltd. is established in **Israel** and hosts the Service in the customer's selected region - **EU (Ireland, eu-west-1)** or **US**. Some of our sub-processors are located in, or transfer data to, the **United States**. Depending on where your data starts, the following safeguards apply:

1. **From the EEA → Aidealy (Israel).** No additional safeguard is required: **Israel has an EU adequacy decision** (Commission Decision 2011/61/EU), so data can flow from the EEA to Aidealy in Israel as it would within the EU.
2. **From the UK → Aidealy (Israel).** No additional safeguard is required: **Israel has full UK adequacy** (a UK "data bridge").
3. **From Israel → our sub-processors abroad.** Carried out under the **Israeli Protection of Privacy (Transfer of Data Abroad) Regulations**: each sub-processor contractually undertakes to apply Israeli-equivalent data-protection conditions and guarantees no unauthorised onward transfer.
4. **To our US sub-processors (the onward "Service sub-processor" leg).** Protected by the **EU Standard Contractual Clauses** (Commission Decision 2021/914), with a UK Addendum for UK data and a transfer impact assessment. Where a US sub-processor also holds a certification under the **EU-US Data Privacy Framework** (or its UK and Swiss extensions), we treat that certification as a **supplementary** protection only - the Standard Contractual Clauses remain our primary safeguard.
5. **Where your data stays in the EU.** If your organisation is on our EU region, your **stored** work data is hosted in the EU and is not transferred to the US merely by being hosted with us; cross-border safeguards apply to the specific onward flows to US sub-processors described above.

The principal such flow is the **AI-model inference leg**, which reaches a US recipient whichever of the two listed AI model providers Aidealy routes a step to: **Anthropic** stores API data in the **United States - never EU-resident** (its API offers no EU-resident option); **OpenAI** today processes at its default **United States** endpoint (its EU regional option is supported in our software but not yet switched on) and, where the analytics assistant is routed to it, stores that assistant's conversation history server-side in the **United States**. In either case the submitted content is a US transfer safeguarded by the Standard Contractual Clauses, and each provider's retention terms are set out in DPA §10. US-based monitoring services are the other onward flow, likewise safeguarded by those Clauses.

For the **account and business-operations providers (Tier B)**, cross-border transfers are covered by those providers' own data-processing agreements, which use the EU Standard Contractual Clauses or another GDPR transfer safeguard (and, where applicable, the UK Addendum), and are described in our **Privacy Policy** rather than the DPA.

The per-sub-processor transfer mechanism for Tier A is set out in **Annex IV of our DPA**.

Contracts and flow-down

Each sub-processor is engaged under a **written contract** that imposes data-protection obligations no less protective than those we owe you, and we **remain responsible to you** for our sub-processors' performance.

- For **work data** (Tier A), this reflects GDPR Art. 28(4): the same data-protection obligations are imposed on each sub-processor by contract, and Aidealy remains fully liable to the customer if a sub-processor fails to meet them.
- For US customers' work data (Tier A), this reflects the CCPA/CPRA service-provider and contractor requirements, including the duty to bind any sub-processor by written contract to the **same level of privacy protection** and to notify the business of such an engagement.

We do not **sell or share** your personal data (as those terms are defined under US privacy law): we disclose data to the providers above only so they can perform their services for us under these contracts; for customer work data (Tier A), this is a service-provider disclosure, not a sale or share.

Publishing this list is a voluntary transparency commitment. Neither the GDPR nor the CCPA/CPRA requires us to publish a named sub-processor list; we do so to give you a complete diligence record. This list is written in English; if we provide a translation for convenience, the English version prevails.

Contact

Questions about this list or our sub-processors:

Aidealy Ltd. privacy@aidealy.ai Hamidron 1, Herzliya, Israel