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

Aidealy IDE Extension - Privacy Notice

Effective date: 2026-11-09 · Version: 1.13.0 · Last updated: 2026-11-09

This Notice explains what the **Aidealy IDE extension** (the "Extension") collects from your development environment, why, where it goes, and the choices you have. It applies to both editions of the Extension - **Aidealy (EU)** and **Aidealy (US)** - installed in **Cursor** or **Visual Studio Code**. The Extension collects the development-activity data described in Section 3.1 from **Cursor** only; it does not collect Claude Code activity. Aidealy's separate **Claude Code collector** - a standalone program that reads Claude Code transcripts - is covered by its own **Aidealy Claude Code Collector Privacy Notice**, not by this Notice.

It is published by **Aidealy Ltd.** ("Aidealy", "we", "us") and is the Extension's data-collection disclosure for the **Visual Studio Marketplace** and **Open VSX**. It is **separate** from the **Aidealy Product Privacy Policy** (which covers the Aidealy web application and your account) and from the **Data Processing Agreement** between Aidealy and your organisation (which sets the contractual data-protection terms for the data described here). The image on the Extension's store page is served from Aidealy's own delivery service, which logs each request; our Website Privacy Policy describes those logs.

1. Please read this first - what the Extension does

The Aidealy Extension measures research-and-development productivity. To do that, it reads data from your IDE - including your **Cursor AI assistant database** - and uploads it to the Aidealy platform for analytics.

You should understand that, in its current default configuration, the Extension transmits the content of your AI-assistant activity - not only metadata. Specifically, it sends the **text of your AI prompts and the AI's responses, code diffs, and repository status** that Cursor stores locally, together with activity metadata. Section 3 describes exactly what is and is not collected. If you do not want this, you can turn the Extension's telemetry off (Section 6).

The first time the Extension runs (and again if this Notice or the licence changes), it shows you a **first-run dialog** that summarises this collection and links to the **Extension EULA** and this Notice. That dialog records your response - your acceptance of the software licence, or your decline or dismissal - as described in Section 3.3; it does not switch collection on or off - the controls in Section 6 do that.

If you decline or dismiss that dialog, collection does not stop. The Extension is deployed by **your organisation**, and the collection described in this Notice rests on your organisation's authorisation as the controller (Section 2) - not on your acceptance in the dialog. What a recorded decline does do: it creates durable evidence that these documents were shown to you and how you responded (Section 3.3), and it means no licence is formed for you to use the Extension in a standalone, personal capacity. The controls that affect collection on your machine are described in Section 6 - switching collection off, or uninstalling the Extension - and Section 4 explains how your organisation's deployment policy interacts with them.

> If you used an earlier version of the Extension or its prior privacy document, note that this Notice corrects it: earlier text stated that source code, file contents, prompts and responses were never collected. That was not accurate for the data paths described below, and this Notice supersedes it.

© 2026 Aidealy Ltd.

2. Who is responsible for this data (our roles)

- **Your organisation is the controller.** Your employer or the organisation that deployed the Extension decides to use it and for what purpose. Under data-protection law it is the **controller** of the developer-activity data the Extension collects, and is responsible for telling you about, and having a lawful basis for, that collection. Aidealy acts as that organisation's **processor** - we process this data **on its instructions**, under our **Data Processing Agreement** with it.
- **Aidealy is the controller of the Extension's own health data.** For the diagnostic and crash-reporting data the Extension sends to keep itself working (Section 3.3), Aidealy decides the purpose and is the controller. The same is true of the record the Extension makes of your response to the first-run legal dialog (also Section 3.3).

If you have questions about why your organisation collects this data, or you want to exercise rights over it, contact your organisation first; we will help (Section 9).

3. What the Extension collects, and what it does not

3.1 Development-activity and AI-interaction data (sent to Aidealy)

The Extension reads your Cursor IDE's local database and your workspace, and uploads the following to the Aidealy backend (the region depends on your edition - Section 8):

Category	What it includes	Purpose
AI prompt & response content	The text of the messages in your Cursor AI chats/agent sessions - your prompts and the assistant's replies	Measure and analyse AI-assisted development
Code diffs & change content	The code differences ("diffs") Cursor records for AI-suggested changes (accepted, rejected or modified), and the Extension's own measurement of the changes made to the tracked files of each repository you work in during an AI session, whichever tool made them, so that code you wrote by hand, in or outside Cursor, is counted as yours.	Calculate AI acceptance/ impact and AI-assisted-vs-human authorship metrics
Repository & git context	Repository and branch name, commit identifier, whether there are uncommitted changes, and the repository status Cursor records (such as which files are changed)	Attribute activity to projects
Workspace metadata	Workspace/folder name, workspace-relative file paths, file types/languages	Aggregate by project and language
Interaction metadata	Message counts, timestamps, session identifiers, durations, completion/acceptance	Usage and productivity analytics, incl. working-time/ effort estimates

Category	What it includes	Purpose
	counts, model and token-usage information	
Message classification	Automated labels for each AI-chat message you type - the kind of work it asks for (for example writing code, fixing a bug, learning), the part of your system it concerns, the quality concern it raises (for example security or performance), and its apparent tone (frustrated, confused, satisfied, excited, neutral) - derived from the **message text only**, read together with up to three of your previous messages in the same session	Work-pattern analytics and per-developer experience analytics
Identity	Your **email address** and your Cursor account identifier, read from Cursor's sign-in record; two installation identifiers the Extension creates on your machine (Section 3.4); and your account name on the code host of each repository you work in (for example GitHub, GitLab, Bitbucket or Azure DevOps), which the Extension looks up from that code host and Aidealy stores with your record (Section 3.4).	Identify your organisation's account and you within it, and attribute work on each repository to the right person

Which repositories' records Aidealy keeps. The Extension collects from every repository it measures. When Aidealy receives a record, it checks whether the repository it came from belongs to your organisation's connected git accounts and is within the scope your organisation has set for analysis; a record from any other repository - a personal project, a repository your organisation has not connected, a folder that is not a repository, or one it has excluded - is discarded when Aidealy processes it and is not stored or analysed. Aidealy keeps only counts of how many records were discarded and of the reasons why, never the name or the address of the repository. A record that touches several repositories is kept if any one of them is within scope. The upload itself is still used to identify you and your organisation. The check is made when the record is processed and is not applied backwards if your organisation later changes its scope. For the historical copy of your Cursor database (the backfill described below), the Extension also sends a list, built on your machine, of the repositories your history refers to: for each one, the folder it lives in on your machine, the repository's name in the form its remote address spells it, and the code host it lives on. Aidealy keeps a whole session, your typed messages in it included, where any repository its code changes belong to is within scope; a session in which no code was changed anywhere, and a session whose repositories cannot be established, are discarded. The uploaded copy of the

database itself arrives whole, before any of this is decided, and is held as Section 10 describes. If your organisation has not connected any git account yet, every record is discarded until it does.

How it is sent. This data is transmitted over an encrypted (HTTPS/TLS) connection; it is not otherwise encrypted or redacted before it is sent, so Aidealy can read its content on receipt and processes it for the analytics purpose above.

Two upload paths. (a) **Ongoing telemetry** - while enabled, the Extension reads new activity from Cursor's database and uploads it. (b) **Historical backfill** - when the Extension is first set up on your machine, it uploads a **copy of your entire Cursor activity database** so your past activity can be analysed. It uploads a fresh copy again if you use the **"Clear Local Data"** command (Section 6), if you run the **Resume Historical Upload** command after that upload has finished, or if the Extension's own local database is lost or has to be rebuilt. Temporary local copies made for the upload are removed from your machine on the schedule in Section 10. **Backfill is a complete copy of that database - except your Cursor sign-in tokens, which the Extension blanks in the copy before upload - and it can include everything else Cursor stored about your AI sessions, including content that ongoing telemetry would have filtered, for your whole history - including activity from before your organisation told you about Aidealy** (your organisation is required to complete its worker notices and any consultation **before** starting the backfill; see Section 4 and the Acceptable Use Policy). **The uploaded copy is held in Aidealy's cloud storage as a file in its own right** until Aidealy erases it after analysing it, or until it expires. Section 10 says how long it is kept, and what an erasure or de-identification request does and does not reach.

3.2 What the Extension does **not** collect

- It does **not** scan your whole disk: it works from Cursor's database and from the repositories open in your workspace (where it measures changes as described in Section 3.1), and it does not upload the content of files you have not changed.
- It does **not** collect keystrokes, clipboard contents, terminal command output, browsing history, or non-IDE activity.
- It does **not** run on remote SSH, WSL, or dev-container hosts: it runs only on your local machine, not on a remote or shared development host.

> **Note on sensitive content.** Because the Extension transmits the content of your AI prompts, responses and code diffs, anything **you** put into a Cursor prompt or that appears in a recorded diff - including a secret, token or password you paste into the chat - may be transmitted. The Extension does **not** currently filter such content out of this path. Avoid pasting secrets into your AI assistant, and see Section 6 to disable telemetry.

3.3 Extension health data and legal-agreement records (Aidealy as controller)

To keep the Extension working, it sends reports of failures (an error, an operation that ran unusually slowly, or data that could not be delivered) to **Sentry**, our error-monitoring provider. A report contains a sanitized error description and stack trace, basic environment information (Extension version, operating system, editor version), device details (such as processor type, memory, language setting and time zone), a reference number shared by the reports sent while the Extension is running, so that they can be linked to each other, and, for upload failures, reference numbers that Aidealy can match to its own record of the upload; it does not report your ordinary activity in the editor, and the Extension does not add your name, email address or computer name to a report. Sentry also records the approximate location (country, state or province, and city) of the IP address a report is sent from. Sentry deletes a report after its retention period, which on Sentry's published plans is at most ninety (90) days, and deletes its backup copies ninety (90) days after they are made. Before a report leaves your machine, credential fields and recognisable file paths are removed from it. The Extension does **not** record "session replays" of your editor. Sentry receives this data in the region matching your edition (Section 8).

Legal-agreement acceptance records (sent to Aidealy - Aidealy as controller). When the first-run dialog (Section 1) shows you the Extension EULA, this Notice, or another legal document, the Extension records your response and sends it to Aidealy - **both acceptances and declines or dismissals** are recorded (for provisioned users; if you are not a provisioned user, your data is not accepted or processed - Section 3.4). Each record is **identity-bound and versioned** and contains: who you are (your email identity) and your organisation/tenant; the versions of the documents shown to you and of those you accepted; the action you took (accept, decline, or dismissal); the date and time; the Extension's version and edition; the **IP address from which your response reaches us** (the network address our servers observe when the record reaches us, which may be later than the moment you acted); an **opaque device identifier** provided by your editor (the human-readable name of your machine is expressly **not** collected); your IDE's type and version; your **operating-system platform** (Windows, Mac, or Linux); and a **content hash of the agreement text displayed to you** together with the dialog's UI version, so that what you were shown can be established later. **If your response was a decline or a dismissal, the record is slimmer: the IP address and the opaque device identifier are not recorded.** Those two fields are collected only when you **accept**, where they help evidence that an agreement was formed; the rest of the record - who you are, your organisation/tenant, the document versions shown, the action, the date and time, the displayed-text hash, and your IDE details - is the same for all responses. A recorded decline or dismissal does **not** switch collection off - Section 1 explains why, and Section 6 describes the controls that do affect collection on your machine. The record is kept **server-side**, in **write-protected, tamper-evident** storage, and is retained for **seven years after the later of** the end of your organisation's relationship with Aidealy **or** your deactivation as a user. Because it exists to establish, exercise or defend legal claims - evidence that the agreement was formed and that you were shown the required notices - it is **not** removed or de-identified by the per-user de-identification described in Section 10, and it survives the end of your organisation's account.

3.4 How we identify you (Cursor sign-in)

Aidealy uses your existing Cursor sign-in to identify you, so your organisation can deploy the Extension without a separate Aidealy account, password, or licence key. To do this, the Extension reads your **email address** and your **Cursor account identifier** from Cursor's local sign-in record and sends them with each upload; it holds no Aidealy sign-in or credential. It also creates two **installation identifiers**: a random identifier for itself (not derived from your hardware or machine name) and an identifier derived from the location of your Cursor settings folder. It sends both with every upload, including your legal-agreement records (Section 3.3), so that records from one installation can be told apart from another. The Extension also looks up your account name on the code host of each repository you work in (for example your GitHub login; on Azure DevOps this is your sign-in address), using the code-host tools or git sign-in already set up on your machine, and sends it to Aidealy so that your work on that repository is attributed to you (Section 3.1); it keeps a local copy so that it does not have to ask again, and it does not send that code-host sign-in to Aidealy. While a backfill upload is held in our cloud storage (Section 10), **that copy holds your cached sign-in email (your Cursor sign-in tokens are blanked in the copy before upload)**, until the copy is erased or expires as described in Section 10. Your Cursor sign-in is provided and governed by **Cursor** under Cursor's own terms and privacy policy; Aidealy only reuses it.

Access is limited so that data is only accepted from authorised users: you must be matched to your organisation's account, through an email address under a domain your organisation has verified or, otherwise, an address an administrator has added to the account and approved; depending on your organisation's settings, an administrator may need to approve you before any data is accepted (until then, that data stays on your device and is retried for a limited time - by default 30 days - after which any still-unsent data is deleted from your device); and each editor sign-in account is linked to a single user in your organisation. If the Extension sends an email address that Aidealy does not yet know, together with a Cursor account identifier already linked to you, that address may be **linked permanently** to your user record. Data flows **one way**: the Extension sends data to Aidealy and does not read your data back from the platform.

For the technical detail of how we check this identity, see the Security & Trust page. Who is responsible for this data, and the legal basis for it, are explained in Section 4.

4. Why we process this data, and the legal basis

Aidealy processes the development-activity data in Section 3.1 **as a processor, on your organisation's instructions**, for the analytics purpose your organisation deployed the Extension for. **Your organisation, as controller, is responsible for the lawful basis** for that processing and for any workplace-information obligations that apply to it (in many places this will be the organisation's *legitimate interests* in understanding R&D productivity, subject to a balancing of your interests - typically not your individual consent, because of the employment relationship). Aidealy processes the Section 3.3 health data as controller on the basis of its **legitimate interest** in keeping the Extension reliable and secure, and the Section 3.3 legal-agreement acceptance records as controller on the basis of its **legitimate interest** in keeping evidence that agreements were formed and required notices were shown, and in establishing, exercising or defending legal claims.

Your device (EU/UK terminal-equipment rules). The Extension stores information on, and reads information from, the computer it is installed on - including the IDE's local database of AI-assistant activity and git repository data - and transmits it to Aidealy on your organisation's behalf. **To measure the code changes it reports, the Extension stores temporary measurement data inside the repository's own version-control storage. It does this for every repository it measures on your machine, including a personal project, and the Extension has no setting that excludes a repository. It never creates commits and never changes your files, branches or stash list.** Where the EU/UK rules on terminal equipment apply (ePrivacy Directive Article 5(3) and national implementations), the required permission for a **work device your organisation provides and controls** is given by **your organisation**, as the subscriber that instructs this deployment; you receive this Notice, the first-run disclosure, and the Section 6 controls so that collection never happens without your knowledge. You can stop collection on your machine at any time, by switching collection off (see the controls in Section 6) or by uninstalling the Extension. Switching collection off stops the Extension reading Cursor's database, stops its uploads and stops it storing the measurement data described above (an upload already in progress completes, the historical upload is not stopped by this switch, and what is waiting on your machine is uploaded if collection is switched back on; see Section 6); uninstalling removes the Extension altogether. Your organisation's policy governs the Extension's deployment, so it may reinstall or re-enable it; the notice and record-keeping described here apply again if it does. **Personally owned (BYOD) devices:** your organisation is required not to enrol a personally owned device unless you have personally agreed to it first, freely and revocably; if the Extension appears on your personal device without your agreement, use the Section 6 controls to stop collection and contact your administrator (or privacy@aidealy.ai).

5. Artificial intelligence, and how your data is (not) used

- **No training on your data.** Aidealy does **not** use the data collected by the Extension to train AI models, and our AI providers, **OpenAI OpCo, LLC** and **Anthropic, PBC** (both described in Section 7), are **contractually committed not to train their models on our customers' content** (**Anthropic**: "Anthropic may not train models on Customer Content from Services"; **OpenAI**: "OpenAI will not use Customer Content to develop or improve the Services, unless Customer explicitly agrees to such use" - OpenAI Services Agreement s. 4.2). **Aidealy has not agreed, and will not agree, to any use of customer content for training.**
- **No solely-automated decisions about you.** Aidealy does not make decisions about you based solely on automated processing that produce legal or similarly significant effects; the analytics are decision-support for human review.
- **Message classification, including tone.** Aidealy automatically classifies each AI-chat message you type: the kind of work it asks for, the part of your system it concerns, the quality concern it raises, and its apparent tone (frustrated, confused, satisfied, excited, neutral). This is **profiling**. It is derived **only from the text you type** (each message is read together with up to three of your

previous messages in the same session, for context only) - not from keystroke timing, voice, face, or any biometric or physiological signal - and is decision-support for human review, never a solely-automated decision about you (see above). It is **not used to infer any health or mental-health condition.** Your organisation can see the resulting labels **per message** - each label with its time and context - but this feature does **not** show your organisation the text of the message a label was derived from. The labels are part of the derived analytics and follow the same retention as the rest of that derived data (Section 10); there is no separate, classification-specific retention period. If you object to this classification, raise your objection with your organisation (Section 9) and Aidealy will assist it in responding. Where your objection is upheld, it is given effect either by your organisation taking the repositories concerned out of its analysis scope, so that records from them are discarded and nothing from them is kept or analysed from that point on (Section 3.1 explains that the check is made when a record is processed and is not applied backwards to records already processed), or by **removing you from collection entirely** (for example, your organisation deactivating your seat or removing the Extension from your machine). There is no setting, for you or for your organisation, that stops the message classification by itself while a repository's records are still analysed.

- **Use to evaluate you, and your rights.** The analytics Aidealy derives about you include an estimate of how much time you spent actively working on your changes (your "effort hours"), how much code you contributed and how it splits between AI-assisted and human-written, and the AI-model usage attributable to you. The estimate is computed in **two variants**, and both may be visible to your organisation. The effort-hours estimate is computed from your **IDE and git activity signals only** - it does not and cannot measure your overall working time, your presence, meetings, reviews, design work, or anything else you do outside those signals, and your organisation is instructed not to use it as a measure of your total working time, presence, or inactivity, **and not to use it as a criterion for deciding your pay, bonuses, or pay progression**. The organisation that provides you with Aidealy may use the analytics to evaluate the performance or behaviour of individual developers, including you, and may use them to help make decisions about you - **including decisions about your pay, bonuses, or pay progression**. The criteria your organisation uses to set your pay are your organisation's own: if you want to know what they are, or how a metric was used in a pay decision about you, **ask your employer** (in some places the law gives you a right to that information - for example, Germany's Pay Transparency Act, and the EU pay-transparency rules as your country implements them). Where your organisation uses the analytics this way, Aidealy is provided as a **high-risk AI system** under the EU AI Act and that organisation is the **deployer**: it must **inform you that you are subject to the system**, apply meaningful human oversight, and **must not make a decision about you based solely on the Service's output** (see above). You keep your data-protection rights, including, in the EEA, the GDPR Article 22 right to human review, to express your view, and to contest a solely-automated decision, and, in the UK, the equivalent safeguards under **UK GDPR Articles 22A to 22D** (the UK's automated-decision rules, which replaced Article 22 on 5 February 2026): to be told about such decisions, to make representations, to obtain human intervention, and to contest them. Similar workplace-AI protections are emerging outside the EU. For example, **Illinois** requires employers to tell employees when AI is used in employment-related decisions. From 2027, **Colorado** adds rights to a disclosure, correction and human review of certain adverse AI-influenced consequential decisions. These are examples, not a complete list. Your organisation, as the deployer/employer, is responsible for the employer-side duties that apply to it. **Korea's** AI Framework Act also imposes AI-transparency duties, but most of those fall on **Aidealy** as the AI operator (see the AI Addendum).
- **Last activity shown to your administrators.** Your organisation's Aidealy administrators can see, for each person on its account, the approximate time Aidealy last received development-activity data from that person.

6. Your controls

Control	How
Turn off all Aidealy product telemetry	Set `aidealy.telemetry.enabled` to `false`. The Extension stops reading Cursor's database and stops uploading; records already waiting, and the commit and settings records it still makes while off, are uploaded if collection is switched back on (see the note below this table).
Turn off Extension health telemetry	Set `aidealy.supportTelemetry.enabled` to `false`.
Use your editor's global setting	If you turn your editor's telemetry **off** (the VS Code / Cursor telemetry setting), the Extension detects that the editor reports telemetry as disabled and automatically switches off **both** product and health telemetry, reacting to changes immediately, with the same effect and the same limits as the first row of this table. This editor setting always overrides the Extension's own settings.
See this disclosure in your editor	Command Palette → **Aidealy: Privacy Settings** - shows a summary of what is collected, with links to this Notice and the Extension EULA.
Export your locally-stored data	Command Palette → **Aidealy: Export Telemetry Data (GDPR)** - exports the Extension's locally-queued data as JSON.
Delete your locally-stored data (this device only)	Command Palette → **Aidealy: Clear Local Data (Right to be Forgotten)** - deletes the Extension's local telemetry database (it keeps the Extension's random installation identifier, Section 3.4). Despite the command's name, this clears **this device only**; it does not delete data already uploaded to Aidealy (see the next row).
Ask for your uploaded data to be de-identified (through your organisation)	Your organisation (the controller) decides whether uploaded development-activity data about you is de-identified - a request from you alone does not trigger it. **Your organisation's Aidealy administrator can perform per-user de-identification directly in the Aidealy Admin application**; that in-product action is your organisation's instruction to us, with no separate written request to Aidealy needed. If you cannot reach your administrator, email privacy@aidealy.ai and we will route your request to your organisation. De-identification has the reach limits described in Section 10.

What switching collection off does, and does not do. Switching collection off stops the Extension reading Cursor's database and stops its uploads: an upload already in progress when you switch it off completes, and the historical upload described in Section 3.1 is not stopped by this switch. Records already queued or staged wait on your machine, and while collection is off the Extension still records the commits you make (their identifier and line counts) and its own settings changes; if collection is later switched back on, those waiting records, the records made while it was off and the Cursor activity recorded on your machine while it was off are all uploaded (records that are never uploaded are deleted from your machine on the queue period in Section 10). Running the **"Clear Telemetry Queue"** command before switching back on deletes only the waiting records; it does not keep out the activity recorded while collection was off. (The broader **"Aidealy: Clear Local Data (Right to be Forgotten)"** command in the table above is the fuller wipe of the Extension's local data.) Uninstalling the Extension ends all collection and staging on your machine.

Your organisation may have configured the Extension for you. Where it manages your machine, for example through a managed machine image or by deploying the Extension's user-level settings for you, it can set these controls on your behalf, and you may find that a control is unavailable to you or that changing it has no effect. A repository's own settings cannot change the collection switch or the local queue retention period. If that happens, contact your administrator.

7. Who we share this data with

We share data only with service providers acting for us (or for your organisation) under contract, and we do **not sell** it or share it for advertising:

- **Amazon Web Services (AWS)** - cloud hosting and storage of uploaded data (including backfill).
- **Functional Software, Inc. (dba Sentry)** - error monitoring (Section 3.3; region per Section 8).
- **AI model providers** - the text of the AI-chat messages you type is sent to a third-party AI model provider for the message classification described in Section 5 (each message with up to three of your previous messages in the same session, as context). Aidealy uses two AI model providers for its AI steps (that classification of your typed messages, the analysis and scoring of source code, and the natural-language analytics assistant, which is the platform's AI analytics chat feature described in Section 10): **OpenAI OpCo, LLC** (an AI model API provider in the United States; it processes this data at its default endpoint; OpenAI's EU regional option is supported in Aidealy's software but not switched on) and **Anthropic, PBC** (an AI model API provider that stores API data in the United States and offers no EU option). 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 adding a provider. Both are named, with their legal entities and processing locations, on our dated Sub-processor List. **Before a provider that is not already named on that list is used for your data, Aidealy tells your organisation at least thirty (30) days in advance, as the Data Processing Agreement requires. That agreement allows one exception: where a provider suddenly becomes unavailable, or has to be replaced urgently to keep the service running or secure, Aidealy may make the change first, must then tell your organisation without undue delay, and your organisation keeps its right to object. If we change the processing location stated here, we update this Notice before the change takes effect; if a provider changes it, we update this Notice as soon as we learn of it. In every case your organisation - as the controller - is responsible for passing the change on to you; we do not rely on you checking the list.**
- The data then flows into the Aidealy platform; additional providers used to operate the platform are listed in our **Sub-processor List**.

Legal process. We may also disclose data to **courts, litigants, and regulatory or law-enforcement authorities** where valid legal process or applicable law compels it, limited to what the process requires. Where such a demand concerns the work data we process for your organisation, the Data Processing Agreement governs how it is handled (including challenging or narrowing overbroad demands, and notice to your organisation where lawful).

No data is shared with advertising networks, data brokers, or AI model-training pipelines.

Business transfers. If Aidealy is involved in a **merger, acquisition, financing, corporate reorganisation, or sale of some or all of its business or assets**, data may be transferred to the **successor entity** when the transaction completes: the development-activity data the Extension collects for your organisation remains governed by the **contract with your organisation (including the DPA)**, which binds any successor to the same obligations, and the limited data Aidealy holds as controller (the Extension health data described in Section 3.3) may be transferred subject to this Notice as in force at the time. During due diligence, any disclosure is limited to the minimum necessary and made under confidentiality obligations; a successor may not materially change how this data is used without the notice (or, where required, the consent) applicable law requires.

8. Where your data is processed (region editions and international transfers)

The Extension ships as **two region-pinned editions**. The **EU edition** sends data to Aidealy's EU region and its error reports to Sentry's EU region; the **US edition** sends them to Aidealy's and Sentry's US regions. **Your edition follows the region your organisation chose** - not your own location. Aidealy is based in **Israel**, and some providers are in the United States.

Where personal data is transferred across borders we rely on recognised safeguards: from the EEA, the European Commission's **adequacy decision for Israel**, and for US providers the **EU Standard Contractual Clauses**, together with the EU-US Data Privacy Framework where the provider holds a live certification; from the UK, the **UK-Israel data bridge** and, for the US, the UK-US data bridge or the UK International Data Transfer Agreement; from Israel, the Israeli Protection of Privacy (Transfer of Data Abroad) Regulations.

> Because the region follows your organisation's choice, **if your organisation selected the US region, your data is processed in the United States even if you are in the EEA or UK.** This transfer is covered by the safeguards described above (Standard Contractual Clauses and, where applicable, the UK Addendum), which are set out in the Data Processing Agreement between Aidealy and your organisation.

Data processed in another country may be subject to that country's laws, including lawful-access requests from its courts, law-enforcement and national-security authorities.

9. Your rights

Depending on where you live, you may have rights to **access**, **correct**, **delete**, **port**, **restrict** or **object to** the processing of your personal data, and to withdraw any consent. Because your organisation is the controller of the development-activity data (Section 2), please direct requests about that data to your organisation; Aidealy, as its processor, will assist it in responding. If you send such a request to Aidealy instead, we will route it to your organisation and **confirm to you that we have passed it on**. For the Extension health data or the legal-agreement acceptance records (Section 3.3), or if you are unsure where to start, contact **privacy@aidealy.ai**. You can also use the controls in Section 6 at any time. **Aidealy will not treat you differently for exercising your rights** (how your organisation treats you is not within Aidealy's control - though retaliation for exercising privacy rights may itself be unlawful under your local law). **If your organisation has ceased to exist or cannot be reached:** where your organisation has ceased to exist without a successor, or has been unreachable for a prolonged period despite our reasonable attempts, we will give effect to your request directly to the extent our systems allow - on an **access** request, by providing you, after verifying your identity and before any de-identification of your records under this fallback, with a copy of your own identity-linked personal data we still hold about you (including the derived analytics); on an **erasure** request, by de-identifying your identity records, to the extent our systems can reach them (Section 10 explains what de-identification does and does not reach) - rather than leaving it unanswered; see the Data Processing Agreement's controller-cessation provision. If you also use the Aidealy web application's AI analytics feature, the conversation history that feature stores is covered by the **Aidealy Product Privacy Policy**, not by this Notice.

10. How long data is kept

- **On your machine:** by default, the Extension's local upload queue is auto-purged after **30 days**, and temporary backfill files are removed after **24 hours**. Both periods are **settings that can be changed** in your editor's settings, in the **Aidealy** section: the queue period can be set from 1 to 90 days and the temporary-file period from 1 hour to 7 days. Where your organisation has configured the Extension for you at machine level, its setting applies instead of yours (see Section 6); a repository's own settings cannot change the queue period, but can set the temporary-file period. These periods govern only the copies held on your own machine; they do not change how long Aidealy keeps data on its platform, which is described below. Local databases are protected by your operating-system file permissions.
- **On the Aidealy platform:** although the Extension *transmits* the content described in Section 3, our backend does **not retain the raw text of your AI prompts and responses at rest in the production analytics stores** (two exceptions on that path: each AI-chat message you type waits in our systems until it has been classified (Section 5), and is then deleted, normally within a few hours; and the historical backfill copy, described in its own bullet below) - that content is otherwise used only **transiently in memory** to compute analytics and is then discarded; code diffs are stored **hash-only**. What we keep is the **derived analytics** (metrics, counts, lengths and hashes). A record from a repository outside your organisation's connected accounts or analysis scope (Section 3.1) is discarded when it is processed and never reaches these stores; the historical backfill copy is the exception described in its own bullet below, because it arrives as a file before that decision can be made. While your organisation is an active customer, that derived data is **kept for the duration of the customer relationship**. Each stored copy of it is deleted **five (5) years after that copy is written** (a copy re-written when Aidealy re-organises its storage starts a new five-year period; a deleted copy's residual storage version is purged within about ninety (90) days after that), and Aidealy reviews these stores at least once a year and deletes records that are no longer needed; the full schedule is in the Data Retention & Deletion Policy. It stays directly searchable for about the first three years of each copy; after that it is moved to lower-cost, non-searchable archival storage. The analytics graph database holds the derived records for the duration of the customer relationship. **When your organisation's agreement with Aidealy ends, its live access to the Service ends with it; its data is kept for a thirty (30)-day window during which your organisation can request a data export (which Aidealy prepares and delivers in CSV/JSON format), and is then permanently deleted from our live systems - including the uploaded telemetry, the derived metrics, and the encryption keys used to protect it** (sooner than the schedule above). Any residual copy still held in our **routine backups** is kept **beyond use** - never restored into active use - and is removed when that backup cycle completes. Separately, the platform's AI analytics (chat) feature keeps its own multi-turn conversation history (held by OpenAI on its servers where the feature is routed to OpenAI; Anthropic holds no server-side conversation state), and a stored conversation can include analytics derived from your activity even if you never use the chat feature yourself. That store belongs to the chat application, not to the Extension; how long it is kept, and how it is deleted, are described in the **Aidealy Product Privacy Policy** (§6) and the **Data Retention & Deletion Policy**.
- **The historical backfill copy of your Cursor database:** the copy the Extension uploads when it is first set up on your machine, and again in the cases described in Section 3.1, is **kept in Aidealy's cloud storage as a file in its own right** - in a storage area that belongs to your organisation, under a folder for you as an individual user (the same storage area also receives the history archives uploaded by Aidealy's separate Claude Code collector, where your organisation deploys it, under their own folders). It is a complete copy of that database, except that **the Extension blanks your Cursor sign-in tokens in the copy before uploading it** (if that blanking step ever fails, the upload still proceeds and the failure is flagged to Aidealy for correction). So for as long as the copy is held it contains your **AI prompts and responses, your code changes, your conversation history and your cached sign-in email**, none of it otherwise filtered. **No one in your organisation - including your administrators - can open or download the copy**: the only

access your organisation's users are ever given to that storage is write-only, for the upload itself, and the only systems allowed to read it are Aidealy's own analysis tasks. **When Aidealy finishes analysing the copy fully successfully, it erases it straight away** - so where a run succeeds fully, the copy exists only for **minutes**. **If the analysis does not fully succeed** - it fails, it cannot process every record, the upload cannot be matched to an uploader, or the deletion step itself fails - **the copy is kept** so the analysis can be retried or diagnosed, and **an automatic expiry rule removes it instead**: the copy is expired **7 days after it is uploaded**, and any superseded version of the same copy is permanently removed within a further **1 day** - so **about 8 days** is the longest any copy can exist. The copy is also destroyed with the rest of your organisation's environment when your organisation's agreement with Aidealy ends (see the bullet above). Nothing else reaches it in the meantime: the Extension's **"Clear Local Data"** command clears your own machine only (Section 6), and a per-user de-identification does not open, edit or delete this copy (see the next bullet). And because the historical upload can run again (for example after you use the **"Clear Local Data"** command, Section 6), a later upload from your machine can again contain content that was previously deleted or de-identified on our platform; each uploaded copy is subject to the same erasure and expiry rules.
- **If your organisation de-identifies you** (for example after you leave): your name and email are replaced in the live application and analytics identity stores, and the record is no longer directly attributed to you there. Some copies sit outside the immediate reach of that action and clear on their own schedules instead: (i) **records in our data lake**, both the uploaded records and the analytics copies made from them (only records from repositories within your organisation's connected git accounts and analysis scope reach it, Section 3.1), which can contain your real name and email, persist until they are deleted on the schedule above; (ii) any **historical backfill copy of your Cursor database** still held in your organisation's upload storage (the bullet above) is not opened, edited or deleted by the de-identification (the bullet above describes what it holds) and is cleared by Aidealy's own erasure when its analysis of the copy fully succeeds, by its expiry schedule, or when your organisation's environment is torn down; (iii) **routine backups** are deleted on the backup schedule in the Data Retention & Deletion Policy (Aidealy's own copies of the account database within about 105 days after they are taken); (iv) the **account-security event register** keeps its tamper-evident record of security events - such as your IDE user being added, which carries your email - as security evidence; (v) the **legal-agreement acceptance record** (Section 3.3) is kept, unedited, for the period stated in Section 3.3, as evidence to establish, exercise or defend legal claims; and (vi) if your IDE **keeps sending telemetry after de-identification**, the platform automatically creates a new, active record carrying your email address and a display name taken from it, until your organisation deactivates the source. The text of the messages you type is sent to one of the two AI model providers named in Section 7 for the message classification described in Section 5 (each message with up to three of your previous messages in the same session, as context). Aidealy does not store that message text at rest in the production analytics stores: it waits in our systems until it has been classified, and is then deleted, normally within a few hours (the backfill copy in item (ii) is the other exception, on its own expiry), and the provider may retain it for a limited period under its own terms (for operational and abuse-monitoring purposes), under the contract we have in place with it.

11. Security

Data is transmitted over **HTTPS/TLS**. Uploaded data is stored in Aidealy's cloud infrastructure with **encryption at rest** (including per-customer encryption keys) and access controls. The Extension runs only on your local machine (Section 3.2).

If a security incident affects this data. Incidents follow the two roles in Section 2: for the development-activity data Aidealy processes for your organisation, Aidealy notifies **your organisation** (the controller) promptly under the Data Processing Agreement - including for confirmed incidents affecting work data even where no personal data is involved - and your organisation is responsible for any notice owed to you; for the data Aidealy holds as **controller** (the Extension health data and legal-agreement acceptance records in Section 3.3, and the account-

security register's record of your IDE user being added), Aidealy itself notifies the authorities and affected individuals as the applicable law requires. Aidealy's Breach-Notification Commitment describes both routes.

12. Region-specific information

- **EEA / UK:** the controller (your organisation) provides the information required by Articles 13 and 14 of the (UK) GDPR, including the **source** of data not collected directly from you (your use of Cursor on your device, under your organisation's deployment). You may complain to your supervisory authority (in the UK, the **ICO**); we ask you to contact us or your organisation first, and we will acknowledge a privacy complaint within **30 days**. Aidealy's EU representative and UK representative are **being appointed**. Until those appointments complete, you may contact Aidealy at **privacy@aidealy.ai** about anything you would otherwise raise with a representative; their names and EU/UK addresses will be published in this Section on completion.
- **Germany:** if you work in Germany and your workplace has a **works council**, the council's co-determination rights (Works Constitution Act - Betriebsverfassungsgesetz - section 87(1) no. 6) typically apply to a tool like the Extension **before** it is rolled out, because it is technically capable of monitoring performance. Your organisation is responsible for concluding any required works agreement; where one exists, it may give you protections beyond those described in this Notice.
- **Israel:** we handle personal data in accordance with the Protection of Privacy Law, including your rights to **access** and **correct** your data. Under Israeli workplace-privacy law (the National Labour Court's *Isakov* ruling and the Privacy Protection Authority's employee-monitoring positions), **your employer** must have a legitimate, work-connected purpose, use proportionate means, tell you clearly and in advance - in a written policy brought to your attention - what is monitored and why, and obtain your informed consent, before deploying the Extension to monitor your work.
- **United States (incl. California):** the categories above include **identifiers**, **professional/ employment information**, **internet/usage activity**, and the **contents of communications** (your AI prompts/responses). We do **not** sell this data or share it for cross-context behavioural advertising. Some items (sign-in credentials and message contents) are **sensitive personal information**; we use them to provide, operate and secure the service. If you would like to limit our use of your sensitive personal information, contact privacy@aidealy.ai and we will honour that right where it applies to you. US residents also have rights to know, delete and correct.
- **Canada:** your organisation - not Aidealy - decides why and how the Extension processes your information (other than the Extension's own health data, Section 2, for which Aidealy is responsible - contact privacy@aidealy.ai); Aidealy processes it only as your organisation's service provider under a data processing agreement, and your organisation remains **accountable** for it under Canadian privacy law. Your information is stored in the region your organisation selected (the EU or the US, never Canada) - see Section 8 on access by foreign authorities. If you work in **Quebec**: the Extension uses technology that performs **profiling** of you (the automated message classification in Section 3.1, derived from your typed chat messages and used in analytics your organisation can see); this Notice is your information about that technology, and Section 6 describes the controls (including turning the collection off). You may ask your organisation's **person in charge of the protection of personal information** to access or correct your information - a written response is due within **30 days** - and no decision about you is ever made solely by automated means (Section 5). Unresolved concerns can go to the **OPC** (Canada) or the **CAI** (Quebec).
- **Australia and New Zealand:** your organisation decides to deploy the Extension and controls the data it collects; Aidealy processes that data as its service provider under a written data processing agreement, in the region your organisation chose. In **Australia**, your employer's own handling of your employment records may fall within the Privacy Act's employee-records exemption, but that exemption does **not** extend to Aidealy - where the Privacy Act applies to us, you can ask us for **access to and correction of** your personal information, and your organisation remains **accountable** (APP 8) when it discloses your information to us overseas. In **New Zealand**, information we process on your organisation's behalf is treated by law (Privacy Act 2020, s 11) as

held by your organisation - direct access, correction and complaint requests to it first, and we will help. Unresolved complaints can go to the **OAIC** (Australia; complain to the organisation first) or the **NZ Privacy Commissioner**.

13. Marketplace and editor telemetry

This Notice is the Extension's data-collection disclosure for the **Visual Studio Marketplace** and **Open VSX** (which Cursor uses). The Extension respects your editor's telemetry choice: when your editor reports telemetry as off, the Extension switches its own collection and health reporting off regardless of its own settings (Section 6 describes what that stops and what is still sent).

14. Changes to this Notice; language

We will post updates here with a new "Last updated" date and note material changes in the Extension's release notes / CHANGELOG. Please review this Notice after Extension updates. This Notice is written in English; if Aidealy provides a translation for convenience, the English version prevails.

15. Contact

Topic	Contact
Privacy questions	privacy@aidealy.ai
Security vulnerabilities	security@aidealy.ai
AI / fairness concerns	ai-concerns@aidealy.ai
General support	support@aidealy.ai

Aidealy Ltd., Hamidron 1, Herzliya, Israel.