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

Aidealy Claude Code Collector - Privacy Notice

Effective date: 2026-11-09 · Version: 1.7.0 · Last updated: 2026-11-09

This Notice explains what the **Aidealy Claude Code collector** (the "Collector") collects from your computer, why, where it goes, and the choices you have. The Collector is a standalone program that your organisation installs on the machines its developers use with **Claude Code** (Anthropic's coding assistant). It runs in the background as your own operating-system user, starting when you log in.

It is published by **Aidealy Ltd.** ("Aidealy", "we", "us"). It is **separate** from the **Aidealy IDE Extension Privacy Notice** (which covers the Aidealy extension for Cursor and Visual Studio Code - a different program that does not collect Claude Code activity), 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).

1. Please read this first - what the Collector does

The Collector measures research-and-development productivity. To do that, it reads the **conversation transcripts that Claude Code keeps on your machine**, and it uploads them to the Aidealy platform for analytics.

You should understand that the Collector uploads the content of those transcripts, not only metadata, and that it does so thoroughly. As Claude Code writes them, it sends: **every prompt you type and every response the model gives; the full text of the files Claude Code reads and the changes it writes; the output of the commands Claude Code runs, verbatim; the images and documents you paste into a conversation; the code differences your files actually received at the moment of each change; and the version-control context** (repository, branch and commit details). There is **no content filter on the upload path**, by design: if a command you ran printed a credential, or a file Claude Code read contained one, that value is in the transcript and is uploaded with the rest. Section 3 describes exactly what is and is not collected. The text of your prompts also leaves Aidealy's platform for one of the two third-party AI model providers named in Section 7 (either may perform this step, and Aidealy may change which one at any time), which classifies each prompt: what kind of work it asks for, which part of your system it concerns, which quality concern it raises, and its apparent tone.

It collects from every project you use Claude Code in - including personal projects and repositories that are not connected to your organisation - and there is no setting on your machine that leaves a project out. What Aidealy then does with a record depends on the repository it came from. **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 a repository your organisation has excluded - is discarded when Aidealy processes it and is never stored:** it is not written to any Aidealy store and nothing about it is analysed. Aidealy keeps only counts of how many records an upload had discarded and of the reasons they were discarded, 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 Collector's own session, workspace and commit records (Section 3.1) are kept whatever project they came from: they carry no repository address or account name, but they do carry the working folder's name, a folder identifier, session times and, for a commit, its identifier and the counts of files and lines changed. The upload itself is still used to identify you and your organisation, as Section 3.4 describes, and if your organisation has not connected any git account yet, every other record from a repository is discarded until it does. The check is made when the

© 2026 Aidealy Ltd.

record is processed and is not applied backwards if your organisation later changes its scope. It applies to continuing collection and to the one-time history upload (Section 3.3) alike, with one difference for the history upload: the archive your machine sends arrives as a single file and is held, unfiltered, in Aidealy's upload staging store until the analysis erases it or it expires (Section 10), and the records inside it are discarded when that analysis reads them.

On first start the Collector also uploads, once, the history Claude Code still holds on your machine - every transcript that exists on the day it is installed, including conversations from before your organisation told you about Aidealy and conversations in personal projects. No setting switches this one-time upload off and opting out does not stop it, but the Collector has a command that cancels it; Section 3.3 says how, and by when.

When the Collector is installed on a machine with you at it, and again whenever the text of that notice changes, it prints a **first-run notice** in your terminal summarising this collection and naming this Notice and the Collector EULA by their web addresses, and asks **"Continue? Answering y confirms you have read this notice and accept the licence terms. [y/N]"**. Your answer is recorded (Section 3.5). **It does not switch collection on or off: if you decline, collection does not stop.** The Collector 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. A recorded decline creates durable evidence that you were shown this Notice and how you responded, and it means no licence is formed for you to use the Collector in a standalone, personal capacity under the Collector EULA. **If the Collector was set up without anyone present**, it shows you the same notice the first time it sees you working in Claude Code: it opens a page in your web browser (served from your own machine) with a button to accept, or, if no browser can be opened, writes the notice into its own log. Either way it records, and sends to Aidealy, that the notice was opened or logged, whether or not you answer (Section 3.5). Closing the page is not a decline, and you can answer later (Section 6). On such a machine the one-time history upload, and the ordinary collection that follows it, do not begin until the notice has been shown to you or logged. When this Notice or the Collector EULA changes, the Collector shows you the notice again in a page in your browser or in its log, whether or not you were at the machine when it was installed. The controls that actually affect collection on your machine are in Section 6.

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

- **Your organisation is the controller.** Your employer or the organisation that deployed the Collector decides to use it and for what purpose. Under data-protection law it is the **controller** of the development-activity data the Collector 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 record of your first-run notice** (Section 3.5) - your answer to it, or the fact that it was opened in your browser or written to the Collector's log: Aidealy decides to keep that record, and why.
- **Aidealy is the controller of the Collector's failure reports.** To keep the Collector working, it reports failures on your machine (for example an upload it could not deliver) to our error-monitoring provider (Section 7). A report carries the Collector's version, your operating system, what failed, how serious it was and where in the Collector's own program code it happened, a few technical numbers about the failure (such as counts, sizes, durations and status codes), the Collector's runtime and configured region, and reference numbers that link it to other reports from the same run and can link it to Aidealy's own record of a request; it does not include your prompts, files, command output, file or repository names, credentials, or your name, email address, organisation's name or computer name. Sentry also records the approximate location (country, state or province, and city) of the IP address a report is sent from. A machine on which nothing fails sends nothing, apart from, at most once a day, a report that the Collector's previous run was stopped before it finished closing (for example by a shutdown). 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. You can switch this reporting off, and opting out of collection switches it off as well (Section 6).

- **Aidealy is the controller of the logs of its download service** (Section 3.6).

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 Collector collects, and what it does not

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

The Collector reads the Claude Code transcript store on your machine (the folder where Claude Code keeps its conversation transcripts, including the transcripts of the helper agents it runs) and, for the repositories you work in, the version-control data needed to measure your changes. It uploads the following to the Aidealy backend (the region depends on the Collector's configuration - Section 8):

Category	What it includes	Purpose
AI conversation content	The text of your prompts and the model's responses, and the system and tool records Claude Code writes into the transcript (which can show the tools and extensions set up for it)	Measure and analyse AI-assisted development
Files and changes	The full text of the files Claude Code reads; the changes it writes, including the changed lines of source; and the code differences your working files received at the moment of each change	Calculate AI-assisted-vs-human authorship and the impact of changes
Command output	The output of commands Claude Code runs, verbatim	Measure and analyse AI-assisted development
Pasted images and documents	Images and documents you paste into a conversation	Part of the transcript; analysed as conversation content
Repository and git context	Repository name (from its remote address), branch, commit details (commit identifier, files changed, lines added and removed), and, where fetched, your account name on the code host	Attribute activity to projects and repositories
Workspace and session metadata	An identifier for the folder you were working in (a one-way hash of its path) and the folder's own name (its last part only, never the whole path); the transcript records themselves are uploaded as Claude Code wrote them, so	Usage and productivity analytics, incl. working-time/ effort estimates

Category	What it includes	Purpose
	a folder or file path Claude Code recorded inside a record is uploaded with that record; session identifiers, timestamps, the Claude Code edition and version, the Collector's own version, tool names, and counts	
Message classification	Automated labels for each prompt 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**, your organisation's identifier, an account identifier, the **git email configured in the repositories you work in**, your code-host account name, and an installation identifier the Collector generates on your machine - read from the sources described in Section 3.4	Identify your organisation's account and you within it

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. The Collector holds **no Aidealy sign-in or credential**: it identifies you by an identity block it composes on your machine from the sources in Section 3.4, and the Aidealy backend checks that block against your organisation's records before accepting any upload.

Two upload paths. (a) **Continuous collection** - the Collector checks the transcript store on a schedule and uploads new records as Claude Code writes them; records wait on your machine until your identity is resolved (Section 3.4) and are retried until delivered or until the local limits in Section 10 remove them. (b) **One-time history upload** - described in Section 3.3.

3.2 What the Collector does **not** collect

- It does **not** read or send your **Anthropic sign-in credential** or the credentials file, and it does not itself open the operating-system keychain: where it looks up your code-host account name it

uses git's own credential mechanism, which may itself use the keychain, and it does not read a credential directory or query the keychain directly. Inside Claude Code's transcript store it opens **only** the transcript files and the small files that accompany them, and nothing else there. Outside that store it reads only the identity sources in Section 3.4, the version-control data of the repositories you work in (Section 4), and Claude Code's store of previous file contents, which it reads on your machine and does not upload.

- It does **not** collect Claude Code's **memory folder** (the notes you or Claude Code keep there), Claude Code's **offloaded tool-output files**, or Claude Code's **store of previous file contents** (which the Collector reads locally to compute differences and does not upload).
- It does **not** scan your whole disk, and it **does not read** another operating-system user's files on the same machine.
- It does **not** collect keystrokes, clipboard contents or browsing history, and it does not record what you do in any other application. Apart from the identity sources in Section 3.4 and the version-control data of your repositories (Section 4), it reads nothing outside Claude Code. **One thing it does record outside Claude Code:** in projects it has seen you use Claude Code in, it regularly checks for new commits and records each one (commit identifier, files changed, lines added and removed - Section 3.1), whether or not Claude Code was involved in making it.

Note on sensitive content. Because the Collector uploads the content of your Claude Code conversations, file contents and command output, anything **you** put into a Claude Code conversation, anything in a file Claude Code reads, and anything a command prints - including a secret, token or password - **is transmitted with the rest of the transcript**. The Collector does **not** filter such content out. Keep secrets out of the files and commands you use with Claude Code, or opt out.

3.3 The one-time history upload

About five minutes after it is installed (or straight away, if it first starts later than that), and in any case not before the first-run notice has been shown to you or written to the Collector's log (Section 1), the Collector uploads a **single archive of the transcripts Claude Code still holds on your machine** (the main and helper-agent transcripts and their small link files - not the previous-file-contents store, and no credential file). How far back that reaches depends on Claude Code's own retention setting on your machine (the first-run notice shows the figure it read); a conversation you resumed keeps its whole history, however old, so the reach can be longer than that setting suggests. **The archive includes everything on the machine at that moment - conversations from before your organisation told you about Aidealy, and conversations in personal projects.** Alongside it the Collector sends a list, built on your machine, of the repositories those conversations belong to. For each repository the list carries the folder it lives in on your machine, the repository's name in the form its remote address spells it (for example `your-organisation/your-project`), and the code host it lives on. The remote address itself is not sent, and any sign-in details it might have contained are removed before the name is taken from it. Aidealy uses that list to apply the same rule as to continuing collection (Section 1) when it processes the archive: records from repositories outside your organisation's connected accounts and analysis scope are discarded before anything is stored, and a record whose folder the list does not cover is discarded too. The archive file itself is held in Aidealy's upload staging store until the analysis erases it or it expires (Section 10). Your organisation is required to complete its worker notices and any consultation **before** starting collection (see Section 4 and the Acceptable Use Policy). Opting out does not stop this upload and no setting switches it off, but **you can cancel it**: running `aidealy-claude-code-collector backfill cancel` stops it, and the cancellation lasts until you run the resume action yourself. Cancel it before the upload starts - about five minutes after installation on a machine with you at it, or, on a machine set up without anyone present, before the first-run notice has been shown to you or written to the Collector's log (Section 1) - and nothing is uploaded at all; cancel it later and what has already been sent has been sent. Not installing the Collector, or removing it

before it runs, has the same effect. The upload runs **once per installation**, and live collection starts only after it has finished, been cancelled or stopped after repeated failures.

3.4 How we identify you

The Collector has no Aidealy sign-in. It works out who you are from what is already on your machine, and the Aidealy backend then matches that to a person in your organisation's account. **Not every source applies in every case**: the Collector uses the first source that yields an identity, and which sources come into play depends on how you sign in to Claude Code. The sources are:

1. **A settings file your organisation's IT may manage** on the machine (Claude Code's managed-settings file and its drop-in folder), which can name your email address and your Claude account and organisation identifiers.
2. **Your Claude sign-in**: the Collector asks Claude Code's own command-line tool who is signed in, and reads, from Claude Code's configuration file on your machine, your email address, account identifier, organisation identifier, organisation name and role, and the time that profile was refreshed. It reads nothing else from that file. The organisation name and role are shown to you locally and are not sent.
3. **Your cloud sign-in**, only if the sources above name no one and you use Claude Code through AWS, Azure or Google Cloud: the Collector asks the provider's own command-line tool for the signed-in identity (an email-shaped user name, plus your organisation's account, tenant or project identifier). It reads no cloud credential files.
4. **The git email configured in each repository you work in** (or your global git configuration, or the `GIT_AUTHOR_EMAIL` or `EMAIL` environment variables as fallbacks), sent together with the repository's host and provider type with every upload from that repository. This address is used only to **match** you to a person your organisation's account already knows; **it never creates a new user record**.
5. **Your account name on the code host** (for example your GitHub login), which the Collector fetches about once a day from the code host's own service using the git credential already stored on your machine, for the major hosting providers only.

The Collector also creates a **random installation identifier** for itself (not derived from your hardware or machine name) and an identifier derived from the location of your Claude Code configuration folder, and sends both with every upload so that records from one installation can be told apart from another.

What happens on the Aidealy side. Your uploads are accepted only for your organisation's account: if the domain of your email address is one your organisation has verified, you are matched to your organisation; otherwise an upload is accepted only if an administrator has already added your exact address to the account. Where your organisation uses **automatic provisioning** and your email domain is verified, **a user record (and a seat) is created for you on your first accepted upload, without any administrator action**; where it uses manual approval, or where your address is outside a verified domain, an administrator must approve you before any data is accepted. Until you are matched and approved, your data stays on your machine and is retried. If the Collector sees a second email address for you from the same installation, that address may be **linked permanently** to your user record. Where your organisation has connected its GitHub organisation, Aidealy also checks your address against the **verified-domain member list** of that organisation the first time you are seen; an address it cannot match is recorded with your organisation's account records as an address that could not be matched, so that your organisation can resolve it. **There is no screen for this today, so nobody in your organisation sees that record; it is kept, with your full address in it, until it is cleared as described in Section 10.**

Data flows **one way** - the Collector sends data to Aidealy and does not read your data back; the only things it receives are the upload links it needs, the backend's answer to each upload, such as whether it was accepted or should be tried again later, and the update file and any new version of the Collector from Aidealy's download service (Section 3.6). *Section 11 describes how the backend*

checks this identity. Who is responsible for this data, and the legal basis for it, are explained in Section 4.

3.5 The record of your first-run notice (Aidealy as controller)

When the first-run notice (Section 1) asks you to confirm that you have read it and accept the licence terms, and you answer **yes or no** - by typing your answer in the terminal, or, for a yes, by pressing the accept button on the notice page - the Collector records your answer and sends it to Aidealy as a legal record. **When the notice is opened in a page in your browser (Section 1), the Collector records, as the page opens, that the notice page was opened, and sends that record to Aidealy, whether or not you then answer on the page**; where no browser could be opened and the notice was written into the Collector's log instead (Section 1), it records and sends that the notice was written to the log. Such a record is not an acceptance and not a decline: it establishes only that the notice page was opened in your browser, or that the notice was made available on your machine, at that time. If you answer, on the page or later, your answer is sent to Aidealy as a separate record: in Aidealy's records, the record that the notice was opened or written to the log never replaces an answer you have given and is never replaced by one (on your machine the Collector keeps a single record for the document versions in force: your answer, once you have given one). If you interrupted the terminal prompt, or the input ended before you answered, that non-answer is recorded on your machine and is not sent. Until the notice has been shown to you or written to the log in one of the ways Section 1 describes, nothing is recorded. Each record is **identity-bound and versioned** and contains: who you are (the identity block described in Section 3.4); the versions of this Notice and of the Collector EULA that the notice referred to; your answer, or the fact that the notice was opened in your browser or written to the Collector's log; the date and time you answered, or at which that happened; the Collector's version and configured region; the Claude Code application and version you were using; your **operating-system platform** (Windows, Mac or Linux); and a **content hash of the exact notice text displayed to you** together with the text's version, so that what you were shown can be established later. **If you accepted**, the record also carries the installation identifier and the **network address from which the record reaches us** (the address our servers observe at delivery, which may be later than the moment you answered); **those two fields are recorded only on an acceptance: a decline, and a record that the notice was opened or written to the log, do not carry them.** A recorded decline, or a record that the notice was opened or written to the log, does **not** switch collection off - Section 1 explains why. 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. The same period applies to every kind of record described in this Section, including a record that the notice was opened or written to the log, each of which exists to establish, exercise or defend legal claims. Aidealy uses these records for nothing else: they play no part in the analytics your organisation sees, and no part in any evaluation of you. You can object to Aidealy keeping a record about you (Section 9); Aidealy will assess your objection, and may keep the record where it is needed to establish, exercise or defend legal claims. Because it exists to establish, exercise or defend legal claims, 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.

3.6 Automatic updates

Except on a Mac where your organisation's IT team installed the Collector for every user, while it runs the Collector regularly asks Aidealy's download service whether a new version is available, and downloads and installs it from there when one is offered. You and your organisation can turn off the installing (Section 6), but the check continues so that the Collector can show when a new version is available; Section 6 also says how to stop the check. The request carries no development data and no identity value. Aidealy's download service logs the date and time, the IP address the request comes from, the country, the file requested, the name and version of the software making the request and technical details of the connection.

You can object to Aidealy keeping these logs about you (Section 9).

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 Collector 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 failure reports in Section 2 as controller on the basis of its **legitimate interest** in keeping the Collector reliable and secure, and the Section 3.5 record of your first-run notice - your answer, or the fact that the notice was opened in your browser or written to the Collector's log - as controller on the basis of its **legitimate interest** in keeping evidence that required notices were shown and agreements were formed, and in establishing, exercising or defending legal claims. It processes the logs of its download service (Section 3.6) as controller on the basis of its **legitimate interest** in keeping that service secure and investigating misuse.

Your device (EU/UK terminal-equipment rules). The Collector stores information on, and reads information from, the computer it is installed on - including Claude Code's transcript store, the identity sources in Section 3.4 and the version-control data of the repositories you work in - and transmits it to Aidealy on your organisation's behalf. **To measure the code changes it reports, the Collector stores temporary measurement data inside the repository's own version-control storage. It never creates commits, never changes your files, branches or stash list, and skips repositories you do not own.** It does this in every project it collects from, including personal projects. 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 notice and the Section 6 controls so that collection never happens without your knowledge, and on a machine set up without anyone present the one-time history upload, and the ordinary collection that waits for it, do not begin until the first-run notice has been shown to you or written to the Collector's log (Section 1). You can stop collection on your machine at any time. Opting out (Section 6) stops the Collector reading your transcripts and storing that measurement data, `backfill cancel` stops the one-time history upload, and **uninstalling the Collector stops everything.** If your organisation has locked those settings, contact your administrator. **Personal projects and personally owned devices:** because the Collector reads every project you use Claude Code in, it can reach repositories that belong to you personally rather than to your organisation. Under our agreement with your organisation it must not put Aidealy's software on a personally owned device unless you have personally agreed to it first, freely and revocably. **That commitment covers the Collector as well as the Aidealy IDE extension.** Your organisation is also required to tell you before rollout that personal projects on an enrolled machine are collected (and discarded by Aidealy's backend when processed, Section 1); if the Collector appears on your personal device without your agreement, opt out (Section 6) 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 Collector 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 prompt 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 prompt 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 the time it was given and the session it belongs to - 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 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 Collector 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 **development-tool 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 and the Collector version last reported.

6. Your controls

Control	How
Opt out of collection entirely	Set `telemetry.optOut` to `true` in the Collector's settings file, run `aidealy-claude-code-collector privacy opt-out`, or set the environment variable `AIDEALY_COLLECTOR_OPT_OUT`. Any one of the three opts you out. From its next collection cycle after you opt out, it stops reading your transcripts and stops storing measurement data in your repositories. **It does not stop everything: the one-time history upload (Section 3.3) still runs, the Collector still checks for new commits in projects it has already seen, it still refreshes your code-host account name, and it still checks for and installs updates. Uninstalling is the only way to stop all of it; on a Mac where your organisation's IT team installed the Collector for every user, ask that team to remove it.** None of the three routes requires an IDE.
Stop the one-time history upload	Run `aidealy-claude-code-collector backfill cancel`. It stops the one-time upload of your existing Claude Code history (Section 3.3) and does not start again on its own; `backfill resume` starts it again and `backfill status` shows where it has got to. Cancelling before the upload begins - about five minutes after installation on a machine with you at it, or, on a machine set up without anyone present, before the first-run notice has been shown to you or written to the Collector's log (Section 1) - prevents it entirely. Ordinary collection is unaffected either way.
Turn off failure reporting	Set `supportTelemetry.enabled` to `false` in the Collector's settings file; your organisation can lock this setting like any other. Opting out of collection (first row) switches failure reporting off as well, and uninstalling stops it with everything else.
Turn off automatic updates	Run `aidealy-claude-code-collector set-auto-update off`. This stops the installing; the check continues (Section 3.6). To stop the check as well, set the environment variable `AIDEALY_COLLECTOR_DISABLE_AUTOUPDATE` where the Collector's background program can read it; it takes effect the next time the Collector

Control	How
	starts. Your organisation can also turn automatic updates off and lock the setting.
Read this disclosure again	Run `aidealy-claude-code-collector privacy` - it prints what the Collector sends, what it never reads, and the addresses of this Notice and the Collector EULA. `aidealy-claude-code-collector agreement` shows the first-run notice again and records a fresh answer; it is also how you answer the notice if you closed the page without answering (Section 1).
See what the Collector is doing	`aidealy-claude-code-collector status` (including whether a setting is locked by your organisation), and a status page available only on this machine; the same local server is where the Collector shows you the first-run notice page (Section 1).
Export your locally-stored data	`aidealy-claude-code-collector export`, followed by the path of the file to write, exports everything queued on this device.
Discard the records waiting to be uploaded (this device only)	`aidealy-claude-code-collector queue-clear` deletes every record the Collector has queued on this device, so nothing still waiting is sent; it deletes nothing else. It does **not** remove the on-device record of your first-run notice (Section 3.5), the code-host account name the Collector keeps in its local database (Section 3.4), or the Collector's local log; `uninstall` removes those (on a Mac where your organisation's IT team installed the Collector for every user, see the Uninstall row). It clears **this device only**; it does not delete data already uploaded to Aidealy (see the last row).
Uninstall	`aidealy-claude-code-collector uninstall` removes the program, its start-at-log-in registration, and, for your user, its settings file, its local database, its queue, its logs, its history-upload working files and the on-device record of your first-run notice; it asks you to confirm first and reports anything it could not remove. It leaves two things in place: the machine-level policy file your organisation deployed, which belongs to your organisation and which only an administrator can change, and the temporary measurement data already stored inside your repositories (Section 4), which the Collector never deletes and which your repository's own routine maintenance clears in its own time. The server-side record of your first-run notice (Section 3.5) is

Control	How
	unaffected. Uninstalling ends all collection on your machine. On a Mac where your organisation's IT team installed the Collector for every user, this command removes nothing and tells you to ask that team, who remove the program; your own Collector folder (its settings file, local database, queue, logs, history-upload working files and the on-device record of your first-run notice) then stays on the Mac until you delete it, as do the two things named above.
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 opting out does, and does not do. Opting out stops the Collector reading your transcripts from its next collection cycle onward, so no new conversation is captured and no new measurement data is stored in your repositories. It does **not** delete what was already collected and uploaded (Section 10 describes what your organisation can de-identify), and records already captured and waiting on your machine **are still delivered** - run `queue-clear` first if you do not want that. Four things opting out does **not** stop: the one-time history upload (Section 3.3), which runs whether or not you have opted out; the commit check described in Section 3.2; the daily refresh of your code-host account name (Section 3.4); and the automatic update check and the installing of updates (Section 3.6). **The history upload has a stop of its own, `backfill cancel` (see the table above). Uninstalling the Collector stops all four.**

*Your organisation may have configured the Collector for you. It can lock **any** setting - including the opt-out and the region - through a machine-level policy file that only an administrator can change, and it can use that file to keep collection switched on. Where its IT team installed the Collector for every user of a Mac, that installation also sets the region. A locked setting is shown in the Collector's status output; if a control has no effect, 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 the upload staging store that receives the one-time history archive (Section 10), and delivery of Aidealy's download service, including its logs (Section 3.6).
- **AI model providers** - the text of your typed prompts is sent to a third-party AI model provider for the message classification described in Section 5 (each prompt with up to three of your previous messages in the same session, as context). Aidealy uses two AI model providers for the AI steps

described in this Notice (that classification, and the platform's AI analytics chat feature described in Section 10, whose answers can draw on analytics derived from your activity): **OpenAI OpCo, LLC** (an AI model API provider in the United States; it processes this data at its default endpoint, and 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.**

- **Functional Software, Inc. (dba Sentry)** - error monitoring: it receives only the failure reports described in Section 2 and the IP address they are sent from, from which it records an approximate location, in Sentry's European Union or United States region matching the region your Collector is configured for (Section 8). Sentry is named, with its legal entity and locations, on our dated Sub-processor List.
- The data then flows into the Aidealy platform; additional providers used to operate the platform are listed in our **Sub-processor List**.

No data is shared with advertising networks, data brokers, or AI model-training pipelines. The Collector itself sends nothing to any analytics provider; the only thing it sends to an error-monitoring provider is the failure reports described in Section 2.

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).

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 Collector 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 failure reports in Section 2, the record described in Section 3.5 and the download-service logs in Section 3.6) 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 (regions and international transfers)

The Collector sends data to the Aidealy region set in its configuration: **Aidealy's EU region by default**, or **Aidealy's US region where your organisation has selected the US region for its account** and configured the Collector accordingly. Your organisation can lock that setting so it cannot be changed on the machine. **The region follows your organisation's choice - not your own location.** The exception is automatic updates (Section 3.6): every Collector contacts the same Aidealy download service, whichever region your organisation chose, and that service's logs are stored in Aidealy's EU region (Ireland). 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 failure reports (Section 2), the record of your first-run notice (Section 3.5) or the download-service logs (Section 3.6), 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:** records waiting to be uploaded are kept in the Collector's local queue for up to **30 days** by default and within a size ceiling, after which the oldest records are removed first; the retention period is a setting (1 to 365 days) that your organisation can lock. The on-device record of your first-run notice (Section 3.5) is kept in the Collector's folder and is never removed by those limits; your code-host account name is kept in the Collector's local database and refreshed about daily; the Collector keeps a local log that does not contain your identity values. These periods govern only the copies held on your own machine. Clearing the queue removes the queued records, and uninstalling removes all of these local copies, except on a Mac where your organisation's IT team installed the Collector for every user: there, that team's removal of the program leaves your Collector folder until you delete it (Section 6). Local files are protected by your operating-system file permissions.
- **On the Aidealy platform:** although the Collector *transmits* the content described in Section 3, our production analytics stores do **not keep the text of your prompts and responses, or the raw**

lines of your source code, at rest - those values are removed from each record when it is written (two exceptions on that path: each prompt you type waits in our systems until it has been classified (Section 5), and is then deleted, normally within a few hours; and the history archive, described in its own bullet below); that content is otherwise used **transiently in memory** to compute analytics, and is then discarded. What we keep is the **derived analytics** (metrics, counts, lengths and hashes) together with **file paths, the type of each change, line counts, git context, session names, tool names and your resolved email address**. A record from a repository outside your organisation's connected accounts or analysis scope (Section 1) is discarded when it is processed and never reaches these stores; the one-time history archive is the exception described in the next bullet, because it arrives as a file before that decision can be made. While your organisation is an active customer, that 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 records, 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 Collector; how long it is kept, and how it is deleted, are described in the **Aidealy Product Privacy Policy** and the **Data Retention & Deletion Policy**.

- **The one-time history archive:** the archive the Collector uploads on first start (Section 3.3) is **kept in Aidealy's upload staging store as a file in its own right** - a storage area that belongs to your organisation, under a folder for you as an individual user (the same storage area also receives the Aidealy IDE extension's uploads, under their own folders). For as long as the archive is held it contains your **prompts, responses, the file contents, command output, pasted material and code differences in those transcripts**, none of it filtered. **No one in your organisation - including your administrators - can open or download the archive**: 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 archive fully successfully, it erases it straight away** - so where a run succeeds fully, the archive exists only for a short time. **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 archive is kept** so the analysis can be retried or diagnosed, and **an automatic expiry rule removes it instead**: the archive is expired **7 days after it is uploaded**, and any superseded version of the same file is permanently removed within a further **1 day** - so **about 8 days** is the longest any archive can exist. The archive 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 Collector's `queue-clear` command clears your own machine only (Section 6), and a per-user de-identification does not open, edit or delete the archive (see the next bullet).
- **Download-service logs (Section 3.6):** about 12 months, after which they are deleted.

- **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, which can contain your email address and the retained fields described above, persist until they are deleted on the schedule above; (ii) any **history archive** still held in your organisation's upload storage (the bullet above) is not opened, edited or deleted by the de-identification, and is cleared by Aidealy's own erasure when its analysis of the archive 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 user being added, which carries your email - as security evidence; (v) the **record of your first-run notice** (Section 3.5) is kept, unedited, for the period stated in Section 3.5, as evidence to establish, exercise or defend legal claims; (vi) the **record of addresses that could not be matched** to your organisation's member list (Section 3.4) is deleted 90 days after the address was first seen (an address still unmatched after that is recorded afresh), or sooner when you are de-identified, and the **identity records** that link your addresses and account identifiers to your user record are kept with your organisation's account records until they are cleared by that de-identification or by your organisation leaving Aidealy; and (vii) if the Collector on your machine **keeps sending data 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 or the Collector is removed. Your prompt text itself is sent to whichever of the AI model providers named in Section 7 is in use at the time, for classification; Aidealy does not store it 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 history archive 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**. The Collector carries **no Aidealy credential**: it identifies you by the identity block described in Section 3.4, which the Aidealy backend checks against your organisation's verified domains, member records and administrator approvals before it accepts anything. Uploaded data is stored in Aidealy's cloud infrastructure with **encryption at rest** (including per-customer encryption keys) and access controls. The Collector runs only on your local machine, as your own user, and its local files are protected by your operating system's file permissions for that user. The Collector's program files are distributed with a **checksum manifest** so that your organisation can verify what it installs.

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 failure reports in Section 2, the record of your first-run notice in Section 3.5, the logs of the download service in Section 3.6, and the account-security register's record of your 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 Claude Code on your device, and the repositories you work in, under your organisation's

deployment). For the failure reports (Section 2), the record of your first-run notice (Section 3.5) and the download-service logs (Section 3.6), Aidealy is the controller, and this Notice, which the first-run notice names by its address and which your organisation gives you before the Collector is installed, is the information Aidealy provides you about them. 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 Collector **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 Collector 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 Claude Code prompts, responses, file contents and command output). We do **not** sell this data or share it for cross-context behavioural advertising. Some items (message contents, and any credential that appears in them) are **sensitive personal information**; we use them to provide, operate and secure the service. **How long we keep each of these categories, including the sensitive personal information among them, is described in Sections 2 and 10.** 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 Collector processes your information (other than the failure reports, the record of your first-run notice and the download-service logs, 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), apart from the download-service logs (Section 8) - see Section 8 on access by foreign authorities. If you work in **Quebec**: the Collector's data feeds technology that performs **profiling** of you (the automated message classification in Section 5, derived from your typed prompts and used in analytics your organisation can see); this Notice is your information about that technology. **Those functions are active for every record Aidealy analyses, and there is no setting that switches the profiling on or off by itself.** Section 6 describes the controls you do have: opting out, cancelling the one-time history upload, and uninstalling. 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 Collector 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. How this Notice reaches you

This Notice is published on Aidealy's website, is printed on demand by the Collector's `privacy` command, and is summarised in the first-run notice the Collector shows you (Section 1). Your organisation is required to give you this Notice, and to complete any worker consultation, **before** it installs the Collector on your machine (see the Acceptable Use Policy).

14. Changes to this Notice; language

We will post updates here with a new "Last updated" date and note material changes in the Collector's release notes. When this Notice or the Collector EULA changes, the Collector shows the first-run notice to you again and records it as Section 3.5 describes. 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.