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

Aidealy Acceptable Use Policy

Effective date: 2026-11-14 · Version: 1.6.0 · Last updated: 2026-11-14

This Acceptable Use Policy (this "**AUP**") sets out the rules for using the Aidealy Service. It is **incorporated into, and forms part of, the Aidealy Master Subscription Agreement / Terms of Service** (the "**Agreement**") between **Aidealy Ltd.** ("**Aidealy**", "**we**", "**us**", "**our**") and the customer that subscribes to the Service ("**Customer**", "**you**", "**your**"). Capitalised terms used but not defined in this AUP have the meanings given to them in the Agreement.

1. Who this AUP binds; relationship to the Agreement

1.1 This AUP applies to **Customer and to all of Customer's Authorised Users**, and to anyone Customer or its Authorised Users permit or enable to access or use the Service. **Customer is responsible for its Authorised Users' compliance with this AUP** and for all activity under its account.

1.2 This AUP **supplements, and does not limit,** the use restrictions in the Agreement (including Section 3 of the Agreement). If there is a conflict between this AUP and the Agreement, the **order of precedence in the Agreement applies** (the Agreement prevails over this AUP except where the Agreement says otherwise).

2. What the Service is

The Service is a **private developer-analytics service, intended for use by organisations and their Authorised Users,** that Aidealy operates over **Customer's own source code and development data, and any repositories Customer selects for processing (see Section 4.2A)**, together with the AI-assisted features described in the Documentation. It is **not a public hosting, publishing, messaging, or content-distribution platform.** This AUP is scoped accordingly: it is about lawful, authorised, and non-abusive use of a service that processes the code and development data Customer submits to it or selects for it.

3. Prohibited conduct

Customer will not, and will not permit any Authorised User or other person to, use the Service:

3.1 Illegal, harmful, or fraudulent activity - for any unlawful, fraudulent, deceptive, or harmful activity; in violation of any applicable law or regulation; or to threaten, incite, promote, or facilitate violence, terrorism, child sexual exploitation or abuse, or other serious harm.

3.2 Infringing or unlawful content - to submit, store, or process as Customer Data any material, or to engage in any activity, that **infringes or misappropriates a third party's intellectual-property rights** (including patent, copyright, trademark, trade secret, or other proprietary right) or that is otherwise unlawful. Customer must have, and must maintain, all rights necessary to submit Customer Data to the Service and to permit Aidealy's processing of it as contemplated by the Agreement.

3.3 Personal data without a lawful basis - to submit or process the personal data of any individual **without a valid lawful basis and the rights and notices required by applicable data-protection law.** Customer will not submit special-category or other highly sensitive personal data except as permitted by the Agreement and the DPA, and will use personal data obtained through the Service only for the purposes for which it was authorised. **In particular, Customer will not submit protected health information (PHI) or other data subject to the US Health Insurance Portability and Accountability Act (HIPAA) to the Service: Aidealy is not a HIPAA business associate and does not offer a Business Associate Agreement**, and responsibility for any HIPAA-regulated data submitted despite this Section is allocated to Customer under the DPA (its Section 3.4).

© 2026 Aidealy Ltd.

3.4 Security, integrity, and unauthorised access - to disrupt, or attempt to disrupt, the integrity, security, or performance of the Service or any related system, network, or data; to gain, or attempt to gain, **unauthorised access** to the Service, to other customers' or users' accounts or data, or to any system or network; or to probe, scan, or test the vulnerability of the Service, or breach or circumvent any authentication, security, or access-control measure, **except under a security-testing programme that Aidealy authorises in writing**.

3.5 Harmful code - to introduce or transmit any **malware, virus, or other harmful or malicious code**, or to use the Service to deliver, host, or control any such code or attack infrastructure.

3.6 Interference, scraping, and excessive load - to **scrape, harvest, or extract data from the Service by automated means** except through interfaces Aidealy expressly provides for that purpose; to place an **undue or excessive burden** on the Service or its infrastructure through automated or high-volume activity; or to circumvent, disable, or exceed any usage limit, rate limit, quota, or other technical or contractual restriction on use of the Service.

3.7 Reverse engineering - to **reverse engineer, decompile, or disassemble** the Service, or attempt to derive its source code, underlying ideas, models, or algorithms, except to the extent this restriction is prohibited by applicable law. **Nothing in this AUP restricts Customer or an Authorised User from modifying an item of Client Software installed on their own machine for their own use, or from reverse engineering it in order to debug those modifications, to the extent the licence of an open-source component included in that Client Software requires that they be permitted to do so** (see Section 3.1 of the Agreement and, for the Aidealy Claude Code collector, Section 4.3 of the Collector EULA).

3.8 Competing products and resale - to use the Service, or any of its output, to **build, train, or improve a competing product or service**, or to copy its features, models, or user interface; or to **resell, sublicense, rent, time-share, or otherwise make the Service available to a third party as a service bureau**, except as expressly permitted in the Agreement.

3.9 Misrepresentation and impersonation - to misrepresent Customer's or an Authorised User's identity or affiliation, to impersonate any person or entity, or to misrepresent an association with Aidealy.

3.10 Spam and unsolicited messaging - to use any messaging, sharing, or output feature of the Service to **send or facilitate the sending of spam or unsolicited bulk or commercial messages**, or otherwise in a way that would violate applicable anti-spam or electronic-marketing laws (for example, the US CAN-SPAM Act, Canada's CASL, or the marketing-message rules of the relevant jurisdiction). The named laws are referenced as the standard of conduct; this is a contractual restriction.

3.11 Re-identification of de-identified data - to **attempt to de-anonymise or re-identify** any individual or any customer from Aggregated Data or any de-identified data made available through the Service.

3.12 Export and sanctions - to use or make the Service available **in violation of applicable export-control or sanctions laws** (including those of the State of Israel, the United States, the European Union, and any other applicable jurisdiction). Customer represents that neither it nor its Authorised Users are located in, or are a national or resident of, an embargoed or restricted territory, or are listed on (or 50% or more owned by a party listed on) any applicable list of restricted or sanctioned parties.

3.13 Competitor access, benchmarks, and competing AI development - (a) if Customer is, or becomes, a **Direct Competitor** of Aidealy, to access or use the Service except with Aidealy's prior written consent, and Customer will not knowingly permit a Direct Competitor of Aidealy to access or use the Service through its account; (b) to **publicly disclose or publish the results of any benchmark, performance, or accuracy evaluation of the Service** without Aidealy's prior written consent - internal testing, evaluation, and oversight of the Service (including the monitoring a deployer carries out under Section 4) are expressly permitted, and Customer's use and disclosure

of the outputs the Service produces for it in ordinary use (its own results, metrics, and reports about its own teams and codebases) are not restricted, provided that this does not permit publishing an evaluation of the Service's accuracy, performance, or quality, however that evaluation is generated or framed; or (c) to use the Service or any of its outputs to **develop, train, fine-tune, or improve an artificial-intelligence model, system, product, or service with functionality substantially similar to the Service**, whether for internal use or for distribution - except an internal classifier or similar internal model used only within Customer's own organisation (including an Affiliate only where that Affiliate uses the Service under the Agreement pursuant to its Section 2.8, and excluding every other Affiliate), not distributed, offered, or made available to any third party, and not used, in whole or in part, as a substitute for the Service (see Section 3.1(g)-(i) of the Agreement).

3.14 Upstream AI-provider policies - to submit content to, or use, the Service's AI features in a way that violates the **usage policies of the AI providers identified on Aidealy's Sub-processor List**, as those policies are published by the providers from time to time. The Sub-processor List identifies, for each AI provider, where its current usage policy is published; the version of a provider's usage policy that applies to particular conduct is the version **in effect at the time of that conduct**. A violation that puts Aidealy's access to an AI provider at risk is a ground for suspension under Section 6.5(e) of the Agreement, and Section 12.2 of the Agreement addresses the losses an upstream cutoff caused by Customer content can create.

3.15 Safety-critical activities - in, or in connection with, any **safety-critical activity**: an activity in which a failure, error, unavailability, or inaccuracy of the Service or its outputs could reasonably be expected to result in death, personal injury, or severe physical or environmental damage - for example, the operation of life-support or other critical medical systems, nuclear facilities, air-traffic control or aircraft navigation or communication systems, weapons systems, or autonomous vehicles. **For clarity, using the Service to analyse the development of software that is itself deployed in safety-critical systems is not, by itself, use of the Service in, or in connection with, a safety-critical activity: this restriction addresses use of the Service or its outputs in the operation, control, or safety function of such an activity.** The Service is a developer-analytics service: it is **not designed or intended for use in safety-critical activities**, and any such use is at Customer's sole risk, with Aidealy's liability for it disclaimed as set out in Section 3.1 of the Agreement.

The restrictions in this Section are in addition to the use restrictions in Section 3 of the Agreement, and the AI-specific restrictions in Sections 4 to 6 below.

4. Responsible use of worker-evaluation features (high-risk AI)

The Service provides software-development analytics - including metrics about individual contributors - and AI-assisted features over Customer's own code and development data. **Aidealy provides the Service as a high-risk AI system** within the meaning of the EU AI Act where it is used to evaluate the performance or behaviour of individuals in a work-related relationship (EU AI Act, Annex III, point 4(b)). The Service may lawfully be used for that purpose, **subject to the responsible-use requirements in this Section and to the human-oversight requirement in Section 6.** If Customer uses the Service to make, or assist in making, decisions about individuals, Customer acts as a **deployer** of a high-risk AI system and is responsible for meeting the deployer obligations that apply to it.

4.1 **Instructions for Use.** Aidealy makes available **Instructions for Use** for the Service's AI features - describing their intended purpose, capabilities, limitations, and the human-oversight measures Aidealy provides - in the **AI Addendum** (in particular its Section 5) and in the further information Aidealy makes available on request. Customer will use the Service **in accordance with those Instructions for Use** and within the Service's intended purpose and stated limitations, and will not repurpose, prompt, or configure the Service for a use outside that intended purpose.

4.2 **Customer's deployer responsibilities.** Where Customer uses the Service, or any output, score, or metric it generates, to monitor or evaluate the performance or behaviour of an individual, or to

make or materially inform decisions affecting the terms of an individual's work-related relationship (including task allocation based on individual behaviour or traits, promotion, discipline, remuneration, or termination), Customer will:

- (a) use the Service in accordance with the **Instructions for Use** and assign **human oversight** of its use to one or more natural persons who have the necessary competence, training, authority, and support (see Section 6);
- (b) **not make a decision about an individual based solely on an output of the Service**, and apply meaningful human review before relying on any output (see Section 6);
- (c) before putting the Service into service or using it at the workplace, **inform - and, where required by applicable law, consult - workers' representatives, and inform the affected workers, that they will be subject to the use of the system**. Customer will complete these notices and any required consultation **before activating data ingestion for the affected individuals - and specifically before starting the historical backfill**, which ingests development history that predates the notice (including activity from before the Service was introduced). **Where Customer deploys the Aidealy Claude Code collector, Customer's worker notices must cover it before it is rolled out.** The collector is a second collection product within the Aidealy client software that Section 4.1 of the Agreement describes (the IDE extension, and any other Aidealy client software that Aidealy makes available to Customer for installation on Authorised Users' machines). It uploads to the Service the transcripts of the Claude Code sessions on the machine (the prompts, the model's responses, the files Claude Code reads and changes, and the output of the commands it runs); on its first start it uploads, once, the Claude Code history already held on that machine, including conversations that predate the notice, and no setting switches that one-time upload off; and, to measure the code changes it reports, it stores temporary measurement data inside those repositories' own version-control storage, under the authorisation in Section 4.1 of the Agreement (storing it creates no commit and alters no working file, branch, or committed history). The Aidealy Claude Code Collector Privacy Notice that Aidealy publishes describes that collection in full. **If ingestion (including a historical backfill) has taken place before a legally required notice or consultation was completed, Section 3.2 of the DPA sets out the remediation available to Customer** (deletion or quarantine of the affected ingested history);
- (d) where the Service is used to make or assist decisions relating to an individual, **inform that individual that they are subject to the use of the system**; and note that the individuals identifiable in the data the Service ingests **are not limited to current employees**: ingested repository and development history can identify **former personnel, contractors, and external contributors (for example, open-source committers whose commits are in Customer's repositories)**, and Customer's transparency obligations under applicable data-protection law extend to those individuals too (in the EEA, GDPR Article 14 - including a documented reliance on Article 14(5)(b) where informing each such individual proves impossible or would involve disproportionate effort, in which case the information must be made publicly available; in the United Kingdom, the corresponding route is UK GDPR Article 14(5)(e), read with Articles 14(6) and 14(7));
- (e) carry out any **data-protection impact assessment** required under applicable data-protection law (in the EEA/UK, GDPR Article 35), using the information Aidealy provides in the Instructions for Use, and ensure a valid lawful basis and the worker-transparency and other obligations required of an employer-controller (in the EEA/UK, including GDPR Articles 13, 14 and 88);
- (f) **monitor** the Service's operation in line with the Instructions for Use, keep the logs the Service generates that are under Customer's control for as long as applicable law requires, and **inform Aidealy without undue delay** of any risk or serious incident Customer identifies in its use of the Service;
- (g) **keep records of its deployer-side oversight** - the human-oversight assignments and reviews under paragraphs (a) and (b), the worker notices and consultations under paragraphs (c) and (d), and any assessments under paragraph (e) - for **at least three (3) years** from the decision or use

they relate to (or longer where applicable law requires); **preserve those records, and provide them to Aidealy on reasonable notice**, where a claim, complaint, or regulatory inquiry involving the Service arises; and **provide the information Aidealy reasonably needs for its own incident- and serious-incident-reporting obligations as a provider without undue delay, and in any event within two (2) Business Days of Aidealy's request** ("Business Day" has the meaning the SLA gives "Business Day");

- (h) where an individual affected by a decision Customer made with the Service's assistance requests it, provide that individual with a **clear and meaningful explanation of the role the Service played in the decision-making procedure and the main elements of the decision**, when and as the corresponding explanation-right obligations under the EU AI Act apply to that use; Aidealy's information pack under AI Addendum Section 5.7 expressly includes the explanation inputs Customer needs for this;
- (i) where an individual exercises a right under applicable pay-transparency or equal-pay law to information about the **criteria used to determine their pay, pay level, or pay progression** (for example, under Germany's Pay Transparency Act, or under the national laws implementing Directive (EU) 2023/970 as they take effect), and an output of the Service is among the criteria Customer used, **be able to identify that criterion and how it was used, and ensure the criteria it uses are objective and capable of justification** as applicable law requires; Aidealy's information pack under AI Addendum Section 5.7 includes the pay-criteria explanation inputs for this; and
- (j) comply with all other obligations that apply to it as a deployer under applicable AI law.

4.2A **Selecting repositories for processing.** The Service processes the repositories Customer selects for it, and ingested repository history identifies the individuals who contributed to it - not only Customer's own personnel (see Section 4.2(d)). Records from a repository that the Aidealy client software sends from an Authorised User's machine are processed only where that repository is within Customer's Connected Git Accounts and Analysis Scope (each as defined in Section 1 of the Agreement): as Section 4.1 of the Agreement provides, a record from any other repository is discarded when the Service processes it, and a Customer that has connected no git account has nothing in scope and receives no repository content from any developer's machine (only the Claude Code collector's own session, workspace and commit records, described in Section 4.1 of the Agreement, are kept). What Customer may select therefore depends on the kind of repository. **Private repositories that Customer owns, whose contributors are Customer's own current and former personnel and contractors, are the normal case** and carry no selection duty beyond the rest of this Section 4. In addition:

- (a) **Public repositories unrelated to Customer.** Customer will **not select for processing a public repository unrelated to Customer**: one that Customer neither owns nor maintains and to which neither Customer nor its personnel have contributed. A public repository that Customer does not own or maintain **but to which Customer or its personnel have contributed** may be selected **only where an announcement meeting the requirements of paragraph (b) is in place in that repository** - whoever published it - including paragraph (b)'s requirements for the linked privacy notice and for how long the announcement must remain in place. For the purposes of this Section 4.2A, Customer **"maintains"** a repository where Customer or its personnel hold **commit or merge authority** over it.
- (b) **Public repositories Customer owns or maintains.** Where Customer selects a **public repository that Customer owns or maintains and that has, or accepts, external contributors**, Customer will first **announce in the repository's public documentation (for example, its README or CONTRIBUTING file) that contributions to the repository are analysed and that contributors are measured**, and will keep that announcement in place **for as long as the repository remains selected and for as long as history ingested from that repository remains available in the Service**. An example formulation Customer may adapt: "*Contributions to this repository are analysed by an automated developer-analytics service operated for [maintainer organisation]. If you contribute, your commits and related development activity may be analysed, and individual contribution metrics about you may be generated. Privacy information:*

[link to the maintainer's privacy notice for contributors]." An announcement published this way **is intended to support** the GDPR Article 14(5)(b) route described in Section 4.2(d) (in the United Kingdom, the UK GDPR Article 14(5)(e) route), for the external contributors whom informing individually proves impossible or would involve disproportionate effort; it is effective for that purpose only where the linked privacy notice contains the information GDPR Articles 14(1) and 14(2) require, and the adequacy of the announcement, of the linked notice, and of Customer's documented assessment under that route remain Customer's responsibility.

- (c) **Private copies of public repositories.** Customer will **not select a private repository, however created (fork, mirror, clone, or import), whose history includes external contributors' activity falling inside the "Backfill Window" purchased for Customer's subscription (as defined in Section 1 of the Agreement) - including history imported after selection (for example through upstream synchronisation)** (the backfill would otherwise process those external contributors' in-window activity). A repository whose imported history wholly predates the start of that window may be selected: that imported history falls outside the window, so no result is computed for it and nothing from it is stored (Section 2.10 of the Agreement). **Whether imported history predates the start of that window is determined by the dates the git provider records for that history (see Section 2.10 of the Agreement). Where an import, rebase, or squash has given that history new provider-recorded dates falling inside that window, the history does not predate the window for this purpose and the repository must not be selected.** A repository selected under this paragraph remains permitted only for as long as no external contributors' in-window history is subsequently imported into it. Where Customer needs a repository with in-window imported history processed, Aidealy support will, on request, try to help Customer scope processing to Customer's own post-import activity; this is assistance only, and not a committed capability of the Service; it is provided as-is and without warranty, and Customer remains responsible for verifying, before selecting the repository, that the resulting scope excludes external contributors' history.

4.3 **Allocation of responsibility; Customer is the employer.** Aidealy provides the Service, the Instructions for Use, and the provider-side measures described in the AI Addendum. The deployer obligations in this Section, and Customer's compliance with applicable AI and data-protection law in its use of the Service, are **Customer's responsibility**. As set out in Section 3.4 of the Agreement, **Customer is the sole decision-maker for all employment and personnel actions** informed by the Service: Aidealy exercises no delegated authority over, and takes no part in, any employment or personnel decision, and does not act as Customer's agent (or as an agent of any employer) in making or communicating such decisions; the worker notices, consultation duties, and any legally required bias audits described in this Section 4 are Customer's own. This allocation does not limit Section 12.3 of the Agreement or any liability of Aidealy that applicable law does not permit to be allocated away. Nothing in this Section permits any use prohibited under Section 5.

4.4 **AI-in-employment and employee-monitoring laws in particular jurisdictions.** Laws in and outside the EU also regulate the use of AI to evaluate individuals, the electronic monitoring of workers, and the making or assisting of employment decisions. Most of them bind **Customer** as the employer or deployer; some place their duties on Aidealy instead (see paragraph (e)). **The jurisdiction summaries in this Section are provided for convenience and general information only; they do not constitute legal advice, they are not exhaustive or a substitute for Customer's own review, and Customer remains responsible for its own legal determinations about its use of the Service.** The responsibilities in Section 4.2 apply to Customer's use of the Service wherever it is used; in addition, where Customer, its Authorised Users, or the individuals whose data is processed are in one of the jurisdictions below, Customer will comply with the requirements of that jurisdiction that apply to it, including:

- (a) **Illinois (US).** An employer that uses artificial intelligence with respect to recruitment, hiring, promotion, renewal of employment, selection for training or apprenticeship, discharge, discipline, tenure, or the terms, privileges, or conditions of employment must **notify the affected employees** of that use, and must not use AI in a way that **has the effect of subjecting**

employees to discrimination on the basis of a protected class, or use **ZIP codes as a proxy** for protected classes (775 ILCS 5/2-102(L)). Customer will provide the required notice before using the Service or its outputs for any of those purposes, and will not combine outputs of the Service with postal-code or similar geographic proxies for protected characteristics.

- (b) **New York City (US).** Using an automated tool to **screen candidates for employment, or employees for promotion,** in New York City in a way that **substantially assists or replaces discretionary decision-making** - relying solely on the tool's output, weighting it more than any other criterion, or using it to overrule conclusions derived from other factors, including human decision-making - makes the tool an "automated employment decision tool" that may not be used unless the employer has first obtained an **independent bias audit** within the prior year, published a summary of its results, and given the required advance notice (NYC Admin. Code §§ 20-870 to 20-872 and the implementing DCWP rules). **Aidealy does not collect or provide the demographic (EEO-1 category) data such a bias audit requires.** Customer will not use the Service or its outputs in that manner for New York City candidates or employees unless Customer has itself satisfied those requirements; using outputs consistently with Section 6 - as one factor among others, weighted no more heavily than the other criteria and subject to genuine human discretion - **may be relevant to whether** a use falls within that definition; the determination is Customer's to make.
- (c) **Colorado (US) - from 1 January 2027.** Colorado's automated-decision-making-technology law (SB 26-189) will apply to technology used to **materially influence a "consequential decision"**, including employment decisions about Colorado employees and job applicants. From that date, a deployer must give a **clear and conspicuous notice** that such technology is in use, provide a plain-language **disclosure after an adverse outcome** (within 30 days), honour the individual's rights to **data correction and meaningful human review** of the decision, and retain the required records for three years. Aidealy makes available the developer-side documentation for these duties in the **AI Addendum** and on request.
- (d) **Texas (US).** Customer will not use or deploy the Service or its outputs **with the intent to unlawfully discriminate** against a protected class (Tex. Bus. & Com. Code § 552.056), and will not use the Service in breach of any other prohibited-practice provision of applicable Texas AI law.
- (e) **South Korea.** Korea's AI Framework Act places its statutory duties on the **AI business operator** - Aidealy - rather than on a business customer that uses the Service internally; Aidealy provides the advance notice and AI-output labelling that Act requires (see the AI Addendum). Customer's responsibilities under this AUP still matter in Korea: maintaining **substantive, non-formalistic human review** of any output that materially affects an individual's rights (Sections 4.2 and 6) **may be relevant to whether** use of the Service falls within that Act's "high-impact AI" classification. A Customer that **re-provides** the Service, or AI products or services built on it, to third parties may itself become an AI business operator with its own duties under that Act; Customer will notify Aidealy before doing so (such resale is in any event restricted by Section 3.8).
- (f) **Works-council and employee-representation regimes (Germany and similar).** If Customer deploys the Service in a jurisdiction with employee-representation laws, Customer is responsible for completing any required employee-representative process **before rollout** (see also Section 4.2(c)). In **Germany**, § 87(1) no. 6 of the Works Constitution Act (**Betriebsverfassungsgesetz, BetrVG**) gives the works council a mandatory co-determination right over the introduction and use of technical systems suitable for monitoring employee behaviour or performance; German courts apply this whenever a system is **objectively capable** of such monitoring, regardless of the employer's intent - a category the Service's developer-activity analytics falls within. Introduction generally requires a **works agreement** (or a conciliation-committee award), and a works council can seek a court order stopping the use of a system introduced without one.
- (g) **US employee-monitoring notice laws.** Several US states require employers to notify employees before electronically monitoring their internet, email, or computer usage. **New York** Civil Rights Law § 52-c requires a private employer with a place of business in New York to give

prior written or electronic notice **on hiring** to employees subject to electronic monitoring, obtain the employee's acknowledgment, and post a conspicuous notice, with civil penalties enforceable by the Attorney General. **Connecticut** (Conn. Gen. Stat. § 31-48d) requires prior written notice of the types of electronic monitoring, which a conspicuous posting can satisfy; **Delaware** (19 Del. C. § 705) requires either a recurring electronic notice or a one-time acknowledged notice before monitoring. Other states and localities may impose similar duties; issuing and documenting any required notices is Customer's responsibility as the employer.

- (h) **Israel.** Israeli law treats technological monitoring of employees as an intrusion on a constitutionally protected privacy right that is lawful only within the framework set by the National Labour Court in *Isakov* (LabA (National) 90/08, *Isakov Inbar*, 2011) and the Privacy Protection Authority's employee-monitoring positions: the monitoring must serve a **legitimate, work-connected purpose**; it must be **proportionate** (the least privacy-intrusive means among the reasonable alternatives); and it must be **transparent** - the employer must adopt a clear written monitoring policy, bring it to the affected employees' attention **before** monitoring begins, state what is monitored and why, and obtain the employees' **informed, freely given consent** (express, written consent on full disclosure for more intrusive monitoring). Consent does not cure a disproportionate or purposeless practice, and collected data may be used only for the disclosed purpose. In addition, under Amendment 13 to the Israeli Protection of Privacy Law, assessment data about an individual's functioning at work can constitute **"specially sensitive information"**, with the heightened duties that classification carries. Customer, as the employer, is responsible for satisfying these requirements before connecting its Israeli developers to the Service; Aidealy cannot satisfy them on Customer's behalf.
- (i) **California (US) - CCPA automated-decisionmaking rules.** California's CCPA regulations, as amended by the California Privacy Protection Agency's automated-decisionmaking-technology (ADMT) and risk-assessment rulemaking, effective 1 January 2026 (Cal. Code Regs. tit. 11; section references in this paragraph are to that title), place their duties on **Customer as the employer** - the CCPA "business" - for its California employees, job applicants, and independent contractors. Using the Service's outputs to **replace or substantially replace human decisionmaking** (§ 7001(e)) for a **"significant decision"** about such an individual - hiring; allocation or assignment of work and compensation, including bonuses; promotion; or demotion, suspension, and termination (§ 7001(ddd)(4)) - is a use of ADMT for which Customer must, **no later than 1 January 2027 for uses already running before that date (§ 7200(b))**: provide a plain-language **pre-use notice** (§ 7220); offer an **opt-out** unless one of the three exceptions in § 7221(b) applies (a **human-appeal route** to a reviewer with authority to overturn the decision; a hiring-assessment exception; or a work-allocation/compensation exception - the latter two available only where the ADMT works for the intended purpose and does not unlawfully discriminate); and honour **access requests** explaining the purpose, logic, and outcome of the ADMT use (§ 7222). Maintaining the substantive human review Sections 4.2 and 6 already require - a reviewer who knows how to interpret the output, weighs it together with other relevant information, and has authority to make or change the decision - **may be relevant to whether** a use involves ADMT at all (§ 7001(e)(1)); the determination is Customer's to make. In addition, and **even where every decision has such a human reviewer**, using automated processing to infer a worker's "performance at work" (or ability, reliability, or behaviour, among others) **based upon systematic observation** of that individual as a job applicant, employee, or independent contractor requires a documented **risk assessment** (§ 7150(b)(4)), on the timing rules of § 7155 (before initiating new processing; for processing already running before 1 January 2026, no later than 31 December 2027). Aidealy processes worker personal data in this context as Customer's **service provider** and assists Customer as set out in the DPA (its Section 13.3), including with ADMT access requests (§ 7222(i)); the information pack under **AI Addendum Section 5.7** includes the inputs Customer needs for these notices and assessments.
- (j) **Connecticut (US) - from 1 October 2027.** Connecticut Public Act No. 26-15 (Substitute Senate Bill No. 5, "An Act Concerning Online Safety"), signed 27 May 2026, regulates **automated employment-related decision technology** in its §§ 7 to 12 (effective 1 October 2026; section

references in this paragraph are to that Act). Technology whose output is a **substantial factor** used to make or materially influence a decision to **hire, promote, discipline, or discharge** an individual, to renew employment, to select for training or apprenticeship, or about tenure or the terms, privileges, or conditions of employment is within that definition; decisions producing only a **nonmaterial** change in job tasks, responsibilities, hours, or work assignments, and decisions made with respect to **workplace health and safety, scheduling and planning, or productivity monitoring**, are outside it (§ 7). That exclusion operates at the level of the decision, not the tool: using an output to make or materially influence a hiring, promotion, discipline, or discharge decision is not excluded merely because the technology is described as productivity monitoring. Where Customer uses such technology for an employee or job applicant **in Connecticut on or after 1 October 2027**, Customer is the **deployer** and must: (i) where the technology is intended to interact with that individual, disclose to them **in plain language** that they are interacting with it, unless a reasonable person would find that obvious (§ 9); and (ii) give that individual, **before the employment-related decision is made**, a **written notice** stating **six** things - that an automated employment-related decision technology has been deployed; the purpose of the technology and the nature of the decision; the **trade name** of the technology; the categories of personal data it will analyse or process and **how that data will be assessed** in reaching a decision; the **sources** of that data; and the deployer's **contact information** (§ 10). Those are Customer's duties as the employer and deployer. Aidealy makes available the developer-side information for these duties in the **AI Addendum** and on request (§ 8); in connection with the disclosures this paragraph describes, neither party is required to disclose a trade secret or information otherwise protected from disclosure by law, provided the person withholding it notifies the person it is withheld from and states the basis (§ 11). Separately, and **from 1 October 2026**: use of such technology is **not a defence** to a Connecticut employment-discrimination complaint, although the commission or court may consider evidence of anti-bias testing and similar proactive efforts (§§ 13 and 14, amending Conn. Gen. Stat. §§ 46a-60(b) and 46a-81c); and an employer serving a federal WARN layoff notice on the Connecticut Labor Department must disclose whether the layoffs relate to its use of artificial intelligence or another technological change (§ 26). Connecticut's separate electronic-monitoring notice duty is described in paragraph (g) and applies in addition. Sections 8 to 11 of the Act are enforced **solely by the Connecticut Attorney General** as an unfair or deceptive trade practice, and create **no private right of action** (§ 12).

- (k) **Pay-transparency and equal-pay laws.** Where Customer uses the Service or its outputs to make or inform decisions about an individual's **pay, bonuses, or pay progression** - a use within the Service's intended purpose (AI Addendum Section 5.1), subject to this Section 4 and Section 6 - equal-pay and pay-transparency laws impose duties on Customer as the employer in addition to the AI-in-employment laws described above. **In the EU**, the principle of equal pay for equal work or work of equal value (Article 157 TFEU) and Directive 2006/54/EC require that **all aspects and conditions of remuneration, and the criteria used in pay-determination systems, be free of direct and indirect sex discrimination** (its Article 4), and once an individual establishes facts from which discrimination may be presumed - for example, a statistical skew in metric-driven pay - **the burden of proof shifts to the employer** (its Article 19), so Customer must be able to justify any pay criterion derived from the Service's outputs on objective, non-discriminatory grounds; **part-time workers may not be treated less favourably than comparable full-time workers solely because they work part-time** unless the treatment is objectively justified, applying the principle of *pro rata temporis* where appropriate (Directive 97/81/EC, Framework Agreement clause 4) - note that the Service's activity-based metrics **can read lower for individuals working part-time or atypical schedules** (AI Addendum Section 5.3), which is why the effort-hours metric must not be used as a pay criterion at all (AI Addendum Section 5.6). **Directive (EU) 2023/970 (pay transparency)** required Member States to transpose by 7 June 2026; as the national implementing laws take effect, employers will owe **objective, gender-neutral pay-setting and pay-progression criteria accessible to their workers**, a worker **right to written information** about their own pay level and average pay levels, **gender-pay-gap reporting** (employers of 250 or more and 150-249 workers: first reports due by 7 June 2027), a **joint pay**

assessment where an unjustified average gap of at least 5% in a category of workers is not remedied within six months, and a **reversed burden of proof where the employer breached its transparency obligations**, unless the breach was manifestly unintentional and of a minor character (its Articles 4, 6, 7, 9, 10 and 18); as of 24 September 2026, **so far as Aidealy has been able to verify**, several Member States, including Italy, Greece, Malta and Slovakia, **had adopted transposition laws**, while Germany, France, Ireland, the Netherlands and Sweden **had not** (the French and Dutch bills were before their parliaments), so Customer must track the implementing law of each Member State in which it employs workers (Ireland already operates gender-pay-gap reporting for employers with 50 or more employees under its own 2021 Act). **In Germany**, in addition, the Pay Transparency Act (Entgelttransparenzgesetz) is in force now: in establishments with more than 200 employees it gives an individual worker a **right to information about the criteria and procedures used to determine their own pay and the pay of a comparator activity**, so where outputs of the Service are among the criteria Customer uses to set pay, those criteria fall within what Customer must be able to disclose; and the works council holds a **mandatory co-determination right over remuneration principles and performance-related pay** (Works Constitution Act, § 87(1) nos. 10 and 11) - a **second co-determination requirement, independent of the monitoring co-determination right described in paragraph (f)** - and under Federal Labour Court case law a pay scheme changed without the required co-determination is ineffective, and employees can claim pay under the last properly agreed scheme. **In the UK**, the Equality Act 2010 implies a sex equality clause into every contract of employment (sections 65 and 66), with the burden shifting to the employer once facts indicating an equal-pay breach are shown (section 136); employers with 250 or more employees must publish annual gender-pay-gap figures, in which **bonus pay - including productivity-linked bonuses - is expressly reportable** (the Gender Pay Gap Information Regulations 2017); and part-time workers are protected on the *pro rata* principle (the Part-time Workers Regulations 2000). **In Israel**, the Equal Pay Law 5756-1996 gives workers of the same employer at the same workplace a right to equal pay for the same work, substantially the same work, or work of equal value; **differentials based on output or quality of work are expressly permitted** where they do not embody sex discrimination, with the employer bearing the burden of justification once comparability is shown, and employers with more than 518 employees owe **annual internal and public pay-gap reports and per-employee notices**. **In the US**, the federal Equal Pay Act (29 U.S.C. § 206(d)) permits a pay differential only under its defenses - including **a system which measures earnings by quantity or quality of production** - and under Title VII a facially neutral pay criterion that causes a **disparate impact** on a protected class must be shown to be **job-related and consistent with business necessity** (42 U.S.C. § 2000e-2(k)); state equal-pay laws (including California, Colorado, Illinois, Massachusetts, New York, and Washington) apply **stricter versions of these defenses** - several require that the justifying factors be job-related, consistent with business necessity, and account for the entire differential, several prohibit relying on salary history, and New York expressly lets a claimant defeat the defense by showing that a facially neutral factor produces a disparate impact, that an alternative practice exists that would serve the same business purpose without producing the differential, and that the employer refused to adopt it - and several states add **pay-data reporting or registration duties and pay-range transparency duties** on employers. For California's automated-decisionmaking rules over compensation decisions, see paragraph (i), which already covers "allocation or assignment of work and compensation, including bonuses"; Colorado's SB 26-189 (paragraph (c)) expressly includes compensation within its "consequential decision" definition, and Connecticut's Public Act No. 26-15 (paragraph (j)) defines a covered employment-related decision to include decisions with respect to "the terms, privileges or conditions of employment" - which Customer should treat as including pay decisions. These duties are **Customer's own as the employer**; Aidealy makes available the developer-side information for these duties - including the pay-criteria explanation inputs under **AI Addendum Section 5.7** and the assessment support under **AI Addendum Section 5.9** - and states in the Instructions for Use that the **effort-hours metric must not be**

used as a criterion for determining an individual's pay, bonuses, or pay progression (AI Addendum Section 5.6).

- (l) **Australia.** Some Australian States and Territories regulate the electronic surveillance of workers. In **New South Wales**, surveillance of an employee at work, including computer surveillance (surveillance by software that monitors or records the information input or output, or other use, of a computer), must not start without written notice to the employee given at least 14 days before it starts (unless the employee agrees to a shorter period, or, for a new employee where surveillance is already running or starts within 14 days, before the employee starts work), indicating the kind of surveillance, how it will be carried out, when it will start, whether it is continuous or intermittent, and whether it is for a specified limited period or ongoing; computer surveillance must also follow a policy of the employer on computer surveillance of which the employee has been notified in advance. Surveillance that does not meet these requirements is covert surveillance, an offence unless authorised by a covert surveillance authority, and no such authority covers monitoring an employee's work performance (Workplace Surveillance Act 2005 (NSW), sections 3, 10, 12, 19 and 20). In the **Australian Capital Territory**, surveillance of a worker (including a contractor or volunteer) in a workplace requires written notice at least 14 days in advance (or within a shorter period the worker agrees) stating the matters that Act lists, good-faith consultation with the worker for at least that period, and, for a device or program capable of being used to record or monitor the input or output of a computer, a policy notified in advance that states how the employer's computer resources may and must not be used, what is logged and who may access it, and how compliance with it is monitored and audited (Workplace Privacy Act 2011 (ACT), sections 13, 14, 16 and 18). **The IDE extension and the Aidealy Claude Code collector record information about the use of the computers they are installed on, which is likely to fall within these definitions;** Customer, as the employer, will complete the required notices, policy and consultation before activating data ingestion for the affected individuals (see Section 4.2(c)). Other States and Territories may impose similar duties. Separately, **from 10 December 2026**, where Customer is an APP entity under the Privacy Act 1988 (Cth) and has arranged for the Service to make, or to do a thing substantially and directly related to making, a decision that could reasonably be expected to significantly affect an individual's rights or interests, using personal information about that individual, Customer's privacy policy must describe the kinds of personal information used and the kinds of decisions concerned (Australian Privacy Principles 1.7 to 1.9); the Privacy Act's employee records exemption can cover an employer's handling of records about its own current and former employees, but not about job applicants, contractors or other contributors (see Section 4.2(d)). Aidealy makes available the developer-side information for these disclosures in the **AI Addendum** (in particular its Section 5.7) and on request.
- (m) **Other laws.** The examples above are not exhaustive, and their details (including implementing rules) change. Customer is responsible for identifying and complying with every AI-in-employment, automated-decision, employee-monitoring, or pay-transparency and equal-pay law that applies to its own use of the Service (Section 4.2(j)), including any duty to notify or consult the affected individuals or their representatives before use.

5. Prohibited AI uses

5.1 The practices in this Section are **prohibited outright and are not permitted even though the Service may otherwise be used to evaluate individuals under Section 4.** Customer will not, and will not permit any Authorised User or third party to, use the Service, or attempt to use its AI-assisted features, for any AI practice that is **prohibited under applicable law**. Without limiting this, Customer will not use the Service (or attempt to repurpose, prompt, or configure it):

- (a) to **infer or recognise the emotions** of any individual in the workplace or in an education setting **on the basis of biometric data** (such as facial expressions, voice, or keystroke dynamics), except where expressly permitted by law for medical or safety reasons;

- (b) for **social scoring** - evaluating or classifying individuals over time based on their social behaviour or personal characteristics in a way that leads to detrimental or unfavourable treatment;
- (c) to deploy **subliminal techniques beyond a person's awareness, or purposefully manipulative or deceptive techniques,** that materially distort a person's behaviour and cause, or are reasonably likely to cause, significant harm;
- (d) to **exploit the vulnerabilities** of an individual or group (including those arising from age, disability, or a specific social or economic situation) in a way that materially distorts behaviour and causes, or is reasonably likely to cause, significant harm;
- (e) for **biometric categorisation** of individuals to deduce or infer protected characteristics such as race, political opinions, trade-union membership, religious or philosophical beliefs, sex life, or sexual orientation; or
- (f) for any other AI practice prohibited under the EU AI Act or any other applicable law (the examples in (a)-(e) are illustrative and not exhaustive).

5.2 Customer will not use the Service to generate, or attempt to generate, content or outcomes that are **unlawful, infringing, deceptive, or harmful**, or that violate the rights of any person. Customer will not use the Service or its outputs to **discriminate unlawfully** against any individual or group, including on the basis of any characteristic protected by applicable law. Customer will not attempt to **circumvent, disable, or defeat any safety, content, or usage control** built into the Service's AI features, nor use those features in any manner inconsistent with their intended purpose or the Documentation.

6. Human oversight; no solely-automated decisions about individuals

Because the Service's AI-assisted features generate outputs using machine-learning models, and those outputs may be inaccurate or incomplete, Customer will assign human oversight to one or more competent natural persons and will apply **meaningful human review** to the outputs before relying on them, and will **not use any output as the sole basis for a decision that produces legal effects concerning an individual, or that similarly significantly affects an individual.** Any such review must be carried out by a person with the authority and competence to change the outcome - including to approve, modify, or override it - who takes into account the Instructions for Use (the intended purpose, capabilities, and limitations of the AI features); a nominal or rubber-stamp review is not sufficient. **Where outputs are applied to many individuals in a single decision cycle - for example, a periodic compensation or performance review round - this review requirement applies to each individual decision: review of the process, of the formula, or of aggregate results alone is not meaningful human review of the decision about an individual.** This requirement is in addition to, and does not limit, Customer's own obligations under applicable data-protection law (including the safeguards that apply to automated decision-making and profiling) and Customer's deployer responsibilities in Section 4.

7. Enforcement and consequences

7.1 **Investigation.** Aidealy may **investigate** any suspected violation of this AUP and take the steps it reasonably considers necessary to address it. Customer will cooperate reasonably with any such investigation.

7.2 **Suspension.** Where reasonably necessary - for a violation of this AUP, a security risk created by Customer's use, or where required to comply with law or to prevent harm to the Service or others - Aidealy may **suspend** Customer's or an Authorised User's access to the Service, in whole or in part, **in accordance with the suspension provision of the Agreement (MSA §6.5).** Aidealy will give reasonable advance notice where practicable, will limit any suspension to what is reasonably necessary, and will restore access promptly once the cause is resolved.

7.3 **Termination.** A material or repeated violation of this AUP is a **material breach of the Agreement** and may lead to termination in accordance with the Agreement's termination provisions (MSA §6.2).

7.4 **Cooperation with authorities.** Aidealy may **disclose information and cooperate with law-enforcement or regulatory authorities** where it is legally required to do so, or where it reasonably believes doing so is necessary to comply with law - in each case consistent with the Agreement, the DPA, and the Privacy Policy. Aidealy may also **disclose information to, and cooperate with, a competent regulator, supervisory authority, or market-surveillance authority in connection with the Service** (for example, an authority supervising Aidealy under AI or data-protection law); any such disclosure is **limited to what is necessary** for the purpose of the cooperation, and Aidealy will **give Customer notice of a disclosure concerning Customer where it is lawful to do so**. Nothing in this Section limits the confidentiality protections of the Agreement in any other respect.

8. Reporting violations

To report a suspected violation of this AUP, contact Aidealy at **legal@aidealy.ai**. Aidealy will review the reports it receives and take the action it considers appropriate.

9. Changes to this AUP

Aidealy may update this AUP from time to time. Because this AUP is incorporated into the Agreement, changes to it are made, notified, and take effect as set out in the Agreement's **"Changes to this Agreement; version binding; records"** provision (Section 15 of the Agreement): the dated version of this AUP in effect at the start of a subscription term governs that term; a change that materially reduces Customer's rights or materially expands its obligations takes effect at the start of Customer's next renewal term, after reasonable advance notice (for example, by email or in-product); and Aidealy maintains dated archives of each published version and will make the version applicable to Customer's subscription available on request. This AUP is written in English; if we provide a translation for convenience, the English version prevails.

10. How to contact us

Aidealy Ltd., **Hamidron 1, Herzliya 4654110, Israel**. AUP reports and legal notices: **legal@aidealy.ai**.