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

Data Processing Agreement

Effective date: 2026-10-30 · Version: 1.12.0 · Last updated: 2026-10-30

This Data Processing Agreement ("DPA") forms part of, and is governed by, the agreement between the customer and Aidealy under which the customer subscribes to the Aidealy service (the "Agreement"). It applies where, and to the extent that, Aidealy processes Customer Personal Data on the customer's behalf in providing the Service. If there is a conflict, this DPA prevails over the Agreement on the subject of the processing of Customer Personal Data; the Standard Contractual Clauses (Section 11 and Annex IV) prevail over this DPA on the subject of restricted international transfers.

- **Customer ("Controller"):** the organisation that has entered into the Agreement.
- **Aidealy ("Processor"):** Aidealy Ltd., a company registered in Israel, at Hamidron 1, Herzliya 4654110, Israel (company registration number 517367066). Privacy contact: privacy@aidealy.ai.

This DPA may be entered into electronically and/or incorporated by reference into the Agreement; no handwritten signature is required for it to be binding.

1. Definitions

Capitalised terms not defined here have the meaning given in the Agreement or in Data Protection Law.

- **"Data Protection Law"** means all laws relating to data protection and privacy applicable to the processing of Customer Personal Data under this DPA, including, as applicable: the EU General Data Protection Regulation 2016/679 ("**GDPR**"); the UK GDPR and the UK Data Protection Act 2018 ("**UK GDPR**"); the California Consumer Privacy Act as amended ("**CCPA**") and other US State Privacy Laws; and the Israeli Protection of Privacy Law and its regulations ("**Israeli PPL**").
- **"Controller", "Processor", "Data Subject", "Personal Data", "Processing", "Personal Data Breach"** and **"Supervisory Authority"** have the meanings in the GDPR (and the corresponding terms - including "business", "service provider", "contractor", "sell", "share", and "consumer" - in the CCPA, and "controller", "holder (מחזיק)" and "database" in the Israeli PPL).
- **"Customer Personal Data"** means the Personal Data that Aidealy processes **on the Customer's behalf** in providing the Service, as described in **Annex I**. It does **not** include the account, authentication and billing data that Aidealy processes as a **controller** to operate the customer relationship - that is governed by the Aidealy Product Privacy Policy, not this DPA.
- **"Sub-processor"** means any third party engaged by Aidealy to process Customer Personal Data.
- **"Standard Contractual Clauses" / "SCCs"** means the standard contractual clauses for the transfer of personal data to third countries annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
- **"UK Addendum"** means the ICO's International Data Transfer Addendum to the EU SCCs.
- **"Service"** means the Aidealy product and services provided under the Agreement.
- **"Data Retention & Deletion Policy"** means Aidealy's published Data Retention & Deletion Policy, as made available by Aidealy and updated from time to time, which states the retention periods and deletion schedules referred to in this DPA.

2. Roles of the parties and scope

2.1 **Roles.** As between the parties, for the Customer Personal Data the **Customer is the Controller** (or is itself a processor acting for a third-party controller) and **Aidealy is the Processor**. Aidealy processes Customer Personal Data only on the Customer's behalf.

2.2 **Subject matter.** The subject-matter and duration of the processing, its nature and purpose, the types of Customer Personal Data, and the categories of Data Subjects are set out in **Annex I**.

© 2026 Aidealy Ltd.

2.3 **Aidealy as Processor only; anti-scope-creep.** Aidealy does not determine the purposes or means of the processing of Customer Personal Data. If Aidealy determines the purposes and means of any processing of Customer Personal Data, it will be a controller in respect of that processing and responsible for it as such. In particular, Aidealy does not use Customer Personal Data - including developer-activity metrics - for its own purposes (except to generate Aggregated Data under §2.4), and **does not use Customer Personal Data or Customer content to train, fine-tune or improve any artificial-intelligence or machine-learning model.**

2.4 **Aggregated and de-identified data.** As permitted by the Agreement, Aidealy may generate aggregated and de-identified data derived from the processing and use that data to operate, secure, support and improve the Service and for benchmarking and analytics, **provided that** such data (a) never includes the Customer's source code, prompts or other Confidential Information in identifiable form; (b) is aggregated and de-identified so that neither the Customer nor any individual can be identified or re-identified from it; and (c) is **never** used to train, fine-tune or improve any AI/ML model. Once data is de-identified so that no individual or Customer can be re-identified, it is no longer Customer Personal Data. For clarity, and as the Agreement states (its Section 8.4): using such data to improve the Service's prompts, configurations, thresholds, and deterministic formulas and rules is within "improve the Service" and is not model training; and **Aidealy does not publish cross-customer benchmarks, league tables, or comparative rankings of its customers or their personnel**. This Section is consistent with, and limited by, the Agreement and Data Protection Law.

3. Processing on documented instructions

3.1 **Instructions.** Aidealy processes Customer Personal Data **only on the Customer's documented instructions**, including with regard to transfers to a third country, unless required to do so by applicable law; in that case Aidealy will inform the Customer of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest. The Agreement, this DPA, and the Customer's configuration and use of the Service are the Customer's complete and final documented instructions; additional instructions must be agreed in writing.

3.2 **Lawfulness of instructions.** The Customer is responsible for the lawfulness of the Customer Personal Data and of the Customer's processing instructions, including having a valid legal basis and providing any notices or obtaining any consents required from Data Subjects (for example, the Customer's developers/employees). The Customer will complete the worker notices and any legally required consultation **before activating data ingestion for the affected individuals - and specifically before starting the historical backfill** (see Section 4.2 of the AUP).

Remediation of pre-notice ingestion. If the Customer confirms to Aidealy in writing - or a competent supervisory authority, works council or comparable body, or court orders or determines - that data ingestion for particular individuals (including the historical backfill) began before a notice or consultation legally required of the Customer had been completed, then, on the Customer's documented instruction, Aidealy will **delete or quarantine the affected ingested history** - including the copies held in Aidealy's analytical work-data stores and historical archive - and will complete that remediation within **thirty (30) days** of the instruction. A Customer confirmation under this paragraph must **state its factual basis in reasonable detail** - identifying the affected individuals or repositories and the ingestion or backfill concerned, and the notice or consultation that had not been completed when ingestion began. Aidealy **may rely on the Customer's confirmation in good faith**, without independent verification, and the Customer will **indemnify Aidealy against losses arising from a confirmation that was materially false** when given. "**Quarantine**" means revoking query and processing access to the affected data so that it is kept beyond use; Aidealy may quarantine first and delete afterwards, and a quarantine satisfies this commitment for so long as the corresponding deletion is still executing. Remediation operates at the granularity of the **Customer's tenant as a whole or of one or more identified repositories**: Aidealy does not commit to isolating a single ingestion run, date span, or other finer-grained subset, and where the affected history cannot be isolated at repository level in every store, Aidealy

may quarantine or delete a broader portion of the Customer's ingested history that contains it. Section 10's deletion mechanics (including the disclosed residual stores and the backups paragraph) apply to a deletion under this paragraph, and a deletion under this paragraph is **expressly subject to Section 10's legal-holds paragraph** (deletion yields, to the narrowest extent necessary, to a documented legal preservation obligation).

3.2A **Devices and terminal-equipment rules.** For each device on which the Customer deploys, or directs the deployment of, the Aidealy client software (the IDE extension, and any other Aidealy client software that Aidealy makes available to the Customer for installation on such devices), the Customer represents and warrants that: **(i)** the device is Customer-issued and Customer-managed, **or** the individual user has personally agreed to the deployment before activation on a genuine, freely given, revocable basis; **(ii)** the Customer has the **legal right and authority to authorise the storage of information on, and access to information stored in, that device**, and that authorisation constitutes any consent required under Article 5(3) of Directive 2002/58/EC (the ePrivacy Directive) and its national implementations, to the extent those rules apply; and **(iii)** the Customer informs the affected users before deployment and does not direct deployment on personally owned devices except as described in (i).

3.3 **Infringing instructions.** Aidealy will **immediately inform the Customer** if, in its opinion, an instruction infringes Data Protection Law.

3.4 **Special-category and criminal-offence data.** The Service is not designed to process special categories of personal data (GDPR Art. 9) or criminal-offence data (Art. 10). The Customer will **not** instruct Aidealy to process such data through the Service, and will not include it in the Service, without first notifying Aidealy in writing and agreeing any additional measures, since such data requires safeguards that are the Customer's responsibility as Controller. **Health data (United States).** Aidealy is **not a "business associate" or a "covered entity" under the US Health Insurance Portability and Accountability Act (HIPAA), does not offer a Business Associate Agreement, and the Service is not designed or offered for processing protected health information (PHI)**. The Customer will not submit PHI, or data subject to HIPAA, to the Service; if the Customer does so despite this Section, that submission is a Customer instruction outside the Service's design, and responsibility for it - including any HIPAA consequence - is allocated to the Customer under this Section and Section 3.2. Aidealy's classification of developers' typed messages (which labels the part of the system a message is about, the kind of work being asked for, any quality concern raised, and the apparent tone) is derived from message **text only** and is **not** designed or permitted to be used to infer any health or mental-health condition; were the Customer to instruct such inference, the resulting data could constitute special-category data under GDPR Art. 9 (cf. CJEU C-184/20 on inferred special-category data) and the safeguards in this Section apply.

3.5 **Requests from public authorities.** If Aidealy receives a request or demand from a government, court, or law-enforcement or regulatory authority for access to or disclosure of Customer Personal Data, Aidealy will: **(a)** promptly notify the Customer of the request **unless legally prohibited** from doing so (and, where a prohibition applies, notify the Customer as soon as the prohibition lapses, and use reasonable efforts to obtain a waiver of it); **(b)** first **redirect the authority to request the data directly from the Customer**, where that is a lawful and available course; **(c)** disclose **only the minimum data legally required** to comply; and **(d)** where it has reasonable grounds to consider the request unlawful or overbroad, use reasonable efforts to **challenge** it (consistent with the standard of Clause 15.2 of the SCCs, where they apply). Aidealy's cooperation with authorities under the Acceptable Use Policy or any other document is subject to this Section for Customer Personal Data. **The same commitments apply, with the same mechanics, where Aidealy receives legal process from a private litigant** - for example, a subpoena, civil document-production order, or discovery demand in litigation to which Aidealy is not a party - **seeking Customer Personal Data**: Aidealy will (a) promptly notify the Customer unless legally prohibited (and notify when the prohibition lapses), (b) redirect the requesting party to seek the data from the Customer where that is a lawful and available course, (c) disclose only the minimum legally required, and (d) use reasonable efforts to

challenge or narrow a demand it reasonably considers invalid or overbroad. **Where a request or demand under this Section sweeps in personal data of Data Subjects who are not parties to the underlying matter** (for example, other developers whose identities, activity, or AI-assistant interactions appear within the records demanded), Aidealy will, in addition, use reasonable efforts to **seek protective treatment for that data** before producing it - for example, a protective order, confidentiality or attorneys'-eyes-only designation, filing under seal, or redaction of the non-party individuals' data - to the extent such treatment is available in the forum concerned. Nothing in this paragraph changes the mechanics of SCC Clause 15 (which addresses requests from public authorities) where the SCCs apply, and the Agreement addresses the costs of Aidealy's compliance as a non-party (Section 15 of the Agreement, "Costs of non-party production").

4. Confidentiality

Aidealy ensures that persons authorised to process Customer Personal Data are bound by an appropriate obligation of confidentiality (contractual or statutory) and process the data only as instructed.

5. Security

5.1 **Measures.** Aidealy implements and maintains appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as required by GDPR Art. 32 and Israeli Data Security Regulations. The measures in place as at the date of this DPA are described in **Annex II**.

5.2 **Evolution.** Aidealy may update the measures from time to time provided the updates do not materially reduce the overall level of security of the Service.

6. Sub-processors

6.1 **General authorisation.** The Customer gives Aidealy **general written authorisation** to engage Sub-processors to process Customer Personal Data, subject to this Section. The Sub-processors authorised as at the date of this DPA are listed in **Annex III**.

6.2 **New Sub-processors and right to object.** Aidealy maintains the current list of Sub-processors and will **notify all active Customers by email** at least **30 days** before a new or replacement Sub-processor begins processing Customer Personal Data. For this purpose, a "**new or replacement Sub-processor**" means a change of the **entity** engaged to process Customer Personal Data: the addition of an entity not on the list, or the replacement of a listed entity by another. It does **not** include routing or re-allocating processing **among entities already on the list**, each acting within its disclosed role and safeguards (including automated failover among the listed AI providers - see the AI Addendum, Section 1.6), and it does not include Aidealy's own processing on its own infrastructure (including AI models Aidealy operates itself, or invokes through an infrastructure service inside Aidealy's own cloud account where the model provider has no access to Customer Personal Data). For clarity, a change in which of the listed AI providers handles a given AI feature of the Service - whether made by Aidealy as a routing choice, on a change of model, or automatically as a fallback when one provider is unavailable - is such a re-allocation among entities already on the list and is not a new or replacement Sub-processor; Annex III and Section 10 describe both providers' locations, safeguards and retention terms so that they hold whichever provider performs a step. Within the notice period the Customer may **object** on reasonable data-protection grounds; an objection must be in writing and must state the **specific data-protection grounds** on which it is based. The parties will work in good faith to resolve the objection - including, where commercially feasible, by Aidealy offering to **continue providing the Service to the objecting Customer without the new Sub-processor** - and if they cannot, the Customer may, as its sole remedy, **terminate the part of the Service that cannot be provided without the Sub-processor**, and Aidealy will refund any prepaid, unused fees for that part.

6.2A **Emergency replacement.** Where a Sub-processor suddenly becomes unavailable, or Aidealy must replace it urgently to **maintain the continuity, security, or integrity of the Service** (for

example, an abrupt termination or restriction of Aidealy's access by an AI provider), Aidealy may engage a replacement Sub-processor **before** the notice period in Section 6.2 has run. In that case Aidealy will: (a) notify all active Customers of the engagement **without undue delay**, identifying the replacement, its role, its processing locations, and the applicable transfer safeguards; (b) ensure the Section 6.3 flow-down obligations are in place **before** the replacement processes Customer Personal Data; and (c) preserve the Customer's **objection right retroactively** - the Customer may object within 30 days of the notice on the terms of Section 6.2, with the same remedy.

6.2B **Intra-group and successor substitution.** Where, following a permitted assignment of the Agreement or a corporate reorganisation (see Section 16.6), Aidealy's obligations are assumed by a successor, and the successor (or a member of Aidealy's or the successor's corporate group) is to perform processing in place of Aidealy or of a listed Sub-processor, that substitution is a change of entity and **remains subject to this Section 6**: the Section 6.2 advance notice will still be given, and the Customer keeps its **right to object, with the same remedy**. The substitution may proceed only where the notice **attests in writing** that: **(a)** the substituting entity is bound, before it processes any Customer Personal Data, by data-protection obligations, technical and organisational measures, and transfer safeguards that are the **same as or stronger than** those applying to the entity it replaces (including the Section 6.3 flow-down and, where applicable, the transfer mechanisms in Section 11 and Annex IV); **(b)** the Customer's tenant **remains in its existing region and no Customer Personal Data is moved between regions** (the region commitment in Annex II is preserved); and **(c)** the protections of this DPA are not otherwise reduced for the Customer. Because those conditions preserve the safeguards unchanged, the parties will handle an objection to such a substitution on a **streamlined basis**: the written-objection, good-faith-resolution, and sole-remedy mechanics of Section 6.2 apply unchanged, and the resolution discussion focuses on whether the conditions attested under this paragraph are in fact met. Nothing in this paragraph removes or shortens the notice or the opportunity to object that Article 28(2) GDPR requires under the Customer's general written authorisation.

6.3 **Flow-down and liability.** Aidealy imposes on each Sub-processor, by a written contract, data-protection obligations **materially equivalent** to those in this DPA (including the Art. 32 security and audit obligations), and **remains fully liable to the Customer** for the performance of each Sub-processor's obligations.

6.4 **Diligence information.** Aidealy selects Sub-processors that provide sufficient guarantees and, on request, makes available the information the Customer reasonably needs to satisfy itself of those guarantees.

7. Assistance with Data-Subject rights

Taking into account the nature of the processing, Aidealy assists the Customer by appropriate technical and organisational measures, insofar as possible, to fulfil the Customer's obligation to respond to requests by Data Subjects to exercise their rights under Data Protection Law (including access, rectification, erasure, restriction, portability and objection). If a Data Subject sends such a request directly to Aidealy, Aidealy will, without undue delay, direct them to the Customer and (unless legally prohibited) inform the Customer.

The mechanics of **per-individual de-identification** (self-service, performed by the Customer's administrator in the Aidealy Admin application) and of **rectification** are described in Section 10. **If the Customer ceases to exist or is persistently unreachable**, Section 10's controller-cessation paragraph applies to Data-Subject requests Aidealy receives.

Assistance window. Where the Customer's documented request identifies the assistance it needs under this Section, Aidealy provides that assistance within **ten (10) Business Days** of the request ("Business Day" has the meaning given in Section 10) - and sooner where the Customer identifies a statutory response deadline that requires it and it is reasonably practicable. This window applies to requests that are **reasonable in volume and cadence**: where requests are **manifestly duplicative or excessive** in volume or frequency, Aidealy may **consolidate them** and provide the assistance for the consolidated set, and the ten (10) Business Day window then runs **from the consolidation**;

Aidealy will tell the Customer when it consolidates. This window governs Aidealy's assistance; the Customer remains responsible for its own statutory response deadlines to the Data Subject.

Objections routed by the Customer. A Data Subject's **objection to processing** (GDPR Art. 21 or an equivalent right) that the Customer routes to Aidealy, or upholds and instructs Aidealy on, is handled as a **documented Customer instruction** under Section 3.1. Where the Customer upholds an objection, exclusion is given effect by **removing the individual from collection entirely** - deactivating the individual's seat and/or signing out or uninstalling the IDE extension for that individual - so that no further data about them is collected, alongside the per-individual de-identification described in Section 10 where instructed. The Service has **no finer-grained processing stop for an individual** (for example, no per-individual stop of a single feature or classification, such as the message classification or its tone label, while collection continues), and none is promised.

8. Assistance with security, breach, DPIAs and prior consultation

Taking into account the nature of the processing and the information available to it, Aidealy assists the Customer in ensuring compliance with its obligations under GDPR Arts. 32-36 - security of processing, personal data breach notification to the Supervisory Authority and to Data Subjects, data protection impact assessments, and prior consultation.

9. Personal Data Breach

9.1 **Notification to the Customer.** Aidealy notifies the Customer **without undue delay after becoming aware** of a Personal Data Breach affecting Customer Personal Data, **and in any event within 72 hours** of becoming aware. For this Section, Aidealy becomes "**aware**" when it has a **reasonable degree of certainty that a security incident has occurred that has led to Customer Personal Data being compromised**; that point does **not** depend on the incident having been confirmed as a "Security Incident" within the meaning of Section 9.5, and a short period of investigation to establish whether an incident has in fact occurred does not postpone it once the reasonable degree of certainty is reached.

9.2 **Content and cooperation.** The notification includes the information then available to Aidealy that the Customer reasonably needs for its own breach assessment and notifications, and Aidealy provides further information and reasonable cooperation as it becomes available. Aidealy's notification is not an acknowledgement of fault or liability.

9.3 **Israeli security events.** Where Aidealy, as a "holder" under the Israeli PPL, is itself subject to a duty to report a severe security event, it will do so as required and cooperate with the Customer.

9.4 **Jointly held data; single notification.** Where the same personal information is held by both parties and applicable law permits a single notification to a regulator or to affected individuals in respect of the same breach (for example, under the Australian Notifiable Data Breaches scheme), the **Customer will lead** that notification to the regulator and to the affected individuals, and **Aidealy will support** the Customer with the information and assistance reasonably required to make it. This allocation does not limit Aidealy's notification duty to the Customer under Section 9.1 or either party's own obligation to notify where applicable law requires that party to do so.

9.5 **Security Incidents affecting work data (with or without Personal Data).** A "**Security Incident**" means a **confirmed accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to Customer Data** processed by Aidealy - including the Customer's work data and Confidential Information (such as source code) - **whether or not Personal Data is affected**. Where a Security Incident materially affects Customer Data but is not (or is not yet confirmed to be) a Personal Data Breach, Aidealy will still **notify the Customer promptly** with the information then available. For **any incident Aidealy notifies under this Section 9**, Aidealy will, once its investigation has concluded, provide the Customer with a **written post-incident summary**: what happened, what data and systems were affected, and the measures taken (and, where relevant, planned) to address the incident and reduce recurrence. This Section does not change the notification standards in Sections 9.1 to 9.4 for Personal Data Breaches.

10. Return and deletion

Retrieval Period (assisted export), then deletion. On termination or expiry of the Agreement - for any reason, including a termination for cause - the Customer's live access to the Service **ends** (save as provided in the "If Aidealy is unreachable and non-performing" paragraph below). For **thirty (30) days** after the effective date of termination or expiry (the "Retrieval Period") the Customer may **request an export of its data** by written notice to Aidealy. On a request made within the Retrieval Period, Aidealy will **execute and deliver an export of the Customer's data - including the developer-activity metrics, scores and other outputs Aidealy derives - in CSV and/or JSON format, within ten (10) Business Days ("Business Day" has the meaning the SLA gives "business day") of the request**. **One standard export run is included at no additional charge**; additional export runs, custom formats, and migration assistance are transition assistance provided as a paid professional service (see "Confirmation of deletion; transition assistance; continuity" below). This assisted export gives effect to the Customer's right of **return** - which the Customer exercises, at its choice, by requesting the export during the Retrieval Period - before deletion. Because the **raw source data originates in, and remains within, the Customer's own systems** (its git provider(s) and the developers' own environments), Aidealy is not required to return raw input data, which the Customer continues to hold; raw git inputs are not included in the export.

After the Retrieval Period (and, where the Customer requested an export within it, after delivery of that export) - or earlier, on the Customer's documented request - Aidealy **permanently and irreversibly deletes** all Customer Personal Data it processes, and deletes existing copies, including copies held by Sub-processors that store Customer Personal Data on Aidealy's behalf - such as **AI-provider conversation history stored server-side** (the analytics assistant's conversation store at OpenAI, where the assistant is routed to it): Aidealy's offboarding procedure deletes the Customer's stored AI conversations through the provider's interface first, and the rest of the environment is torn down only once that deletion has fully succeeded. Once Aidealy deletes them, the provider removes the data from its own systems in line with its published commitments - it states that API data it retains is removed after at most 30 days unless it is legally required to keep it; the provider's own record of each response of that feature is not deleted by that procedure, is retained by the provider for **at least thirty (30) days under its own policy** (a stated minimum, not a promised deletion date), and holds no stored conversation content. The only exceptions are **(i)** aggregated and de-identified data as permitted by §2.4, which Aidealy may retain and use (and which is no longer Customer Personal Data), and **(ii)** records Aidealy is **required or permitted by law to retain**, together with **Aidealy's own security and audit logs and Aidealy's own billing-evidence records** (each held in Aidealy's own systems, not as part of the Customer's environment - the Customer's environment, including its per-tenant access logs, is destroyed at offboarding; the billing-evidence records are the daily, pseudonymous tenant-user billing-snapshot records described in the Data Retention & Deletion Policy; this exception applies to them whether or not any law requires the records to be retained, and already-written daily records are not deleted at offboarding and instead age out individually on their 730-day schedule) kept for the limited periods in the Data Retention & Deletion Policy.

Giving effect to an individual's erasure. Per-individual de-identification is **self-service**: the Customer's administrator performs it **directly in the Aidealy Admin application**, and that in-product action constitutes the Customer's documented instruction under this DPA - no separate written request to Aidealy is needed (a request to privacy@aidealy.ai remains available as a routed fallback and is treated the same way once confirmed by the Customer). Where the Customer so de-identifies an individual (or a Data Subject exercises a valid right to erasure routed through the Customer), Aidealy's systems remove that individual's directly-identifying fields (such as name and email) from the **identity records in its operational systems** - the account store and the analytics graph database - replacing them with a non-identifying placeholder. This is **de-identification, not anonymisation**: to the extent any residual record could still be linked to the individual it remains Customer Personal Data and stays protected by this DPA. In addition, where the individual used the AI analytics feature, an automatic nightly job **deletes that individual's stored chat conversations**

from the AI provider's server-side store (the analytics assistant's conversation store at OpenAI, where the assistant is routed to it) - normally within about a day; that job does not delete the provider's own record of each response, which the provider retains for **at least thirty (30) days under its own policy** (a stated minimum, not a promised deletion date) and which holds no stored conversation content.

This individual-level process is deliberately limited to the identity records and stored conversations described above, and does **not** modify: **(i)** the historical work-data records in Aidealy's analytical stores and their query layer, where the individual's identifying details persist until those records are deleted on the retention schedule in the "Work-data retention and the historical archive" paragraph below or earlier on termination of the Agreement - that scheduled deletion, not the individual-level process, is the mechanism that purges them; **(ii)** Aidealy's tamper-evident **account-security event records**, its write-locked **AI-interaction audit log** (which includes the content of the individual's AI analytics queries and answers, and whose entries are retained for **seven (7) years** each, because the audit log is also Aidealy's **legal-claims evidence record** of what the Service actually delivered - it is kept, on the legal-claims basis (of the GDPR Art. 17(3)(e) class), for the period during which a related legal claim could be brought (in Israel, generally **seven (7) years**), per the AI-interaction audit log row of the Data Retention & Deletion Policy; the individual's identity, where it appears **within that stored content**, persists there for that period), and its write-protected, tamper-evident **register of legal-document acceptances** - the identity-bound legal-evidence register recording each individual's acceptance (or decline) of the Extension End User License Agreement and related legal documents, which Aidealy holds **as a controller** and retains for **seven (7) years after the later of the end of the Customer's relationship with Aidealy and the individual's deactivation**, and its **contest-review notes** - the small, account-side record (held in Aidealy's own systems, not as part of the Customer's environment) noting a human review Aidealy actually performed when a contest of, or objection to, a Service output was routed to Aidealy (the date, what was reviewed, and the outcome), kept so that the promised human intervention can still be evidenced for the period during which a related legal claim could be brought (in Israel, generally **seven (7) years**), and its **tenant-user billing snapshot** - the daily, pseudonymous billing-evidence roster (an internal user code, role, seat type, account status and joined/last-active dates; **no name, no email**) that Aidealy holds **as a controller**, as its own evidence of why each month's bill changed - the stored daily counts are the evidence base from which the invoiced seat quantity can be recomputed; none of them is itself the invoiced quantity, nor the seat-metering record the Agreement provides for - (outside the Customer Personal Data definition; see the tenant-user billing snapshot row of the Data Retention & Deletion Policy): daily records written **before** a de-identification keep the individual's pre-departure roster history, under the retained internal user code, for each record's full **730-day** period - none of which is edited after a de-identification, because each is kept as security or legal evidence: the account-security event records and the AI-interaction audit log are deleted on the schedules in the Data Retention & Deletion Policy, the AI-interaction audit log - notwithstanding its seven (7)-year entry period - is still **deleted in full when the Customer's environment is decommissioned** (no audit-log entry survives the Customer's offboarding), the acceptance register **survives both a per-individual de-identification and the decommissioning of the Customer's environment** for its retention period, the contest-review notes are likewise a small legal-evidence record that survives a per-individual de-identification, is deleted when its period expires, and the billing-snapshot records likewise **survive both** a per-individual de-identification and the decommissioning of the Customer's environment - offboarding does not delete that store; each daily record simply ages out on its own 730-day schedule - with every record class in this paragraph remaining subject to the legal-hold paragraph below (a documented legal hold under this Section reaches every record class in this Section); and **(iii)** residual copies in backups, which are kept beyond use and roll off on the backup cycle below. De-identification also does not stop new data from being collected about the same individual: if a departed individual's development environment continues sending telemetry to the Service, the Service treats it as a new person joining the Customer's team and creates a new, active record carrying their email address and a display name taken from it. The

Customer should therefore revoke a departed individual's access to the Service (for example, uninstalling or signing out the IDE extension) as part of its own offboarding.

Backups. Customer Personal Data held in Aidealy's routine system backups is **access-restricted and kept beyond use** - it is not used for active processing or analytics - and rolls off on Aidealy's ordinary backup cycle (provider database snapshots roll off within days; Aidealy's own backup copies of the account database are permanently deleted within approximately one hundred and five (105) days after they are taken), after which it is overwritten or deleted. Where an individual has been erased or data has been deleted from the live systems, residual copies in backups are not restored into active use and are removed on this cycle; they remain protected by this DPA until deleted. **If Aidealy must restore from a backup for disaster recovery**, erasures and deletions that were completed in the live systems after that backup was taken are **re-applied promptly** following the restoration, so the restoration does not resurrect data the Customer or an individual had already had erased or deleted.

Work-data retention and the historical archive. Customer Personal Data in Aidealy's analytical work-data stores is retained for the duration of the subscription. In Aidealy's analytics data lake, each stored copy of a record is queryable for approximately the first **three (3) years** after it is written, is then moved to an access-restricted, **non-queryable cold archive** (**kept beyond use** - not queried for active processing or analytics), and is deleted **five (5) years after it was written**, the deleted copy's residual storage version being purged within approximately ninety (90) days after that. Where Aidealy re-organises its storage or writes a further internal copy of a record, the resulting copy is subject to the same periods from the date it is written. The analytics graph database holds derived work-data records for the duration of the subscription. Aidealy reviews these stores at least once every twelve (12) months and deletes records that are no longer necessary for the Service. All copies are deleted earlier, in full, on termination of the Agreement (after the Retrieval Period above) and remain protected by this DPA until deleted. An individual erasure request does **not** rewrite these historical records (see "Giving effect to an individual's erasure" above): the retention periods described above, or the earlier termination-driven deletion, are the mechanism that purges them. **Separately, where ingestion preceded a legally required notice or consultation, the remediation commitment in Section 3.2 - deletion or quarantine of the affected ingested history, at the granularity of the Customer's tenant or of identified repositories - applies to these stores notwithstanding the retention schedule above.** The Customer may obtain its data through the assisted export described in this Section, requested during the Retrieval Period, before deletion.

Backfill upload staging. Each Aidealy client product stages an upload of the individual's local history in the Customer's **upload staging store**: one store per Customer, shared by the two products, with a separate area for each product and each individual user; the erasure and expiry rules in this paragraph apply to every upload held there. Where the IDE extension performs a **historical backfill** - on first set-up on the Data Subject's machine, and again where its saved record of the earlier upload has been cleared or lost (as happens when the individual uses the IDE extension's command that clears its local data, or when its local database is lost or has to be rebuilt) or where the individual restarts the upload with the IDE extension's own command for resuming it - it uploads a **verbatim copy of that individual's IDE activity database** to that store. **That upload is not bounded by the Backfill Window or by any other date limit: it covers the whole of the individual's local development-tool history held in that database, including activity predating the Customer's subscription. The IDE extension blanks the individual's IDE session credentials (the IDE's sign-in tokens) in the copy before upload**; a failed blanking is flagged to Aidealy and does not block the upload. For as long as that copy is held it otherwise contains **raw AI prompts and responses, code content, conversation state and the individual's cached IDE sign-in record**, without the filtering applied further down the ingestion pipeline. Where the Claude Code collector performs its **one-time history upload** - once per installation, on its first start - it uploads to the same store a **single archive of the Claude Code conversation transcripts still held on the individual's machine** (the main and helper-agent transcripts and their small link files; no credential

file), together with a list, built on the machine, of the repositories those transcripts belong to. That upload is likewise not bounded by the Backfill Window or by any other date limit: it covers every transcript on the machine at that moment, including conversations from before the Customer's subscription and conversations in personal projects. For as long as the archive is held it contains **the individual's prompts, the model's responses, the full text of the files the tool read, the output of the commands it ran, pasted images and documents, and code differences**, none of it filtered; records from repositories outside the Customer's connected git accounts and analysis scope (Annex I, Part C) are discarded when the archive is processed, so the archive is the one copy of such records the Service ever holds. The rest of this paragraph applies to the archive as it applies to the IDE extension's copy. **When a backfill run completes fully successfully, the Service erases the copy immediately**, so for most uploads the copy exists only for minutes. **In every other case** (for example a failed run, a run that skips an archive already processed, a run that could not process every record, an upload that cannot be attributed to an uploader, or a deletion attempt that fails) **the copy is retained for retry or diagnosis and the automatic expiry rule governs instead**: the storage is **configured with an automatic expiry rule that deletes the copy seven (7) days from upload**, and removes any superseded version of the same object within a further **one (1) day**, so that **approximately eight (8) days** is the outer bound for which the copy is configured to exist (subject to the Legal Holds paragraph of this Section); and it is destroyed in full, with the rest of the Customer's environment, at offboarding under the Retrieval-Period paragraph above. Because a backfill can run again (in the cases stated at the start of this paragraph, which include the individual's own actions on the machine), a subsequent upload from the same machine can again contain content that was previously deleted or de-identified on the platform; each uploaded copy is subject to the same erasure and expiry rules. The individual-level de-identification described above **does not reach this copy**: it is not opened, edited or selectively purged in response to an erasure instruction, and the successful-processing erasure, the expiry rule and the offboarding teardown are the mechanisms that remove it. Aidealy applies to this store the same measures as to the Customer's other stores (Annex II): encryption at rest under the **Customer's own key**, all public access blocked, and access confined to the Customer's tenant. **No Customer user, including a Customer administrator, has read access to that storage**: the only credential ever issued to a Customer user for it is write-only and scoped to that user's own upload, and the only systems with read access to the copy are Aidealy's processing tasks for the two products; access by Aidealy personnel is governed by Annex II.

Rectification. Rectification runs in parallel to the erasure process above, with the same reach: **(i)** an individual's **identity fields** (such as a name or email recorded incorrectly) are correctable by the Customer's administrator directly in the Aidealy Admin application; **(ii)** the **derived analytics are recomputed from the source data as new data is ingested**, so a correction made at the source (for example, in the Customer's git provider or IDE-user records) flows into the outputs computed **from that point forward**; and **(iii)** where an individual **contests the accuracy of a metric, score, or other derived record** that sits in a store Aidealy does not edit, the correction takes the form of the Customer **recording the contest and its own correction decision alongside the output it relied on** (see the AI Addendum, Sections 5.7 and 6, for the explanation and human-review machinery this feeds), with Aidealy providing the information the Customer reasonably needs. The stores that are **not edited** are the same disclosed-immutable stores named for erasure above: the historical work-data records in the analytical stores (purged on the retention schedule in the "Work-data retention and the historical archive" paragraph above, or on termination), the tamper-evident account-security event records, the write-locked AI-interaction audit log, the write-protected register of legal-document acceptances, the contest-review notes, the tenant-user billing snapshot (a contested roster fact follows limb (iii) - the correction is recorded alongside the evidence, not written into the locked records), and residual backup copies.

If the Customer ceases to exist or is unreachable. If the Customer has **ceased to exist without a legal successor**, or Aidealy has been **unable to reach the Customer through its recorded contacts for ninety (90) days despite reasonable attempts**, then: (a) Aidealy will **proceed with the deletion**

schedule in this Section as if the Agreement had terminated on the date Aidealy concluded the Customer had ceased or become unreachable (with the Retrieval Period available to any lawful successor who comes forward within it); and (b) for a Data-Subject request Aidealy receives during that state, Aidealy will **give effect to the request directly to the extent it can do so within this Section's mechanics** - for an **erasure** request, by de-identification of the individual's identity records and, **where stored AI conversations of that individual exist (that is, where the individual used the AI analytics feature and the assistant's server-side conversation store at OpenAI, where the assistant is routed to it, holds conversations of theirs)**, deletion of that individual's stored AI conversations; and for an **access** (or portability) request, by providing the individual, **on a verified request** (verification typically by the individual confirming control of the email address linked to their records, or equivalent evidence of identity) **and before any de-identification of their records under this paragraph**, a copy of their **own identity-linked records held in the Service** (their scores and metrics, and, **where they used the AI analytics feature**, their stored AI conversations), executed through the **same support-executed export machinery** as the assisted export at the start of this Section, with **personal data relating to other individuals** (and Customer data that is not part of the requesting individual's own records) **redacted or removed from the copy before delivery** - rather than leaving the request unanswered, and will document what it did. This paragraph is a **safeguard of last resort**: it does not apply while the Customer is merely slow to respond, and it does not make Aidealy the controller of the data.

If Aidealy is unreachable and non-performing (relief of last resort). If Aidealy is **unreachable through its designated contacts and is materially failing to perform** its obligations under the Agreement, and that state continues for **fifteen (15) Business Days** after the Customer's written notice to Aidealy's designated contacts (the notice addresses stated in the Agreement, including legal@aidealy.ai), then the Customer may **treat the Agreement as terminated** with effect from the end of that period. In that event - and **as its own path, distinct from the assisted export** at the start of this Section - the Customer's **live access to the Service continues for so long as the Service's automated systems remain operational**: those systems operate without Aidealy's manual intervention, and the Customer may **access, export and extract its data using the functionality of the Service** during a window of **thirty (30) days** from the date it so treats the Agreement as terminated, and Aidealy will use commercially reasonable efforts to keep those systems funded and operational through that window. This paragraph is a safeguard of last resort: it does not apply while Aidealy is merely slow to respond, and it operates alongside (and does not reduce) the wind-down continuity commitment below.

Legal holds. The deletion obligations in this Section yield, to the narrowest extent necessary, to a **documented need to preserve specific data for actual or reasonably anticipated legal claims or proceedings** between the parties or involving the Service, **or to any other legal preservation obligation binding Aidealy** (for example, a litigation hold or preservation order in a matter involving a third party, or a statutory preservation duty). A hold must be **specific, documented, and time-bounded** (reviewed at least annually); Aidealy will **inform the Customer** of a hold it applies (unless legally prohibited), and data under hold remains protected by this DPA, is kept beyond ordinary use, and is deleted when the hold ends. **Where data under a hold sits in a Customer environment being offboarded, the scheduled destruction of the per-tenant encryption key at offboarding is deferred** until the hold ends, so that the preserved data remains readable for the preservation purpose; only the data under the hold is preserved on that basis, and the rest of the offboarding deletion proceeds.

Sanctions. If performing any obligation in this Section - including executing or delivering the assisted export, returning data, or continuing the live-extraction window above - or paying a related refund under the Agreement, would cause Aidealy to violate applicable trade-sanctions, export-control, or similar laws (for example, because the Customer, or an entity owning or controlling the Customer, has become a designated, blocked, or otherwise restricted party under such laws), that obligation is **suspended for so long as, and to the extent that, performing it would violate those laws**. The Agreement's sanctions provisions (its Section 15) contain the parties' continuing

sanctions representation and Aidealy's suspension and termination rights on a designation; during a suspension under this paragraph Aidealy will **hold, dispose of, or delete the affected data as applicable law, or an applicable licence or authorisation, requires or permits**, and the data remains protected by this DPA until deleted.

Confirmation of deletion; transition assistance; continuity. On the Customer's written request, Aidealy will provide **written confirmation** that the deletion described in this Section has been carried out. On request before or during the Retrieval Period, Aidealy will provide **reasonable transition assistance beyond the one standard export run** described in this Section (for example, additional export runs, custom export formats, or assisted transformation or migration of the Customer's data) as a paid professional service, **at the rates and scope stated in the Order Form or, failing that, at reasonable, documented time-and-materials rates** - the one standard export run itself is included in the subscription. **If Aidealy ceases operations entirely**, Aidealy commits that the assisted export under this Section remains available - and will use **commercially reasonable efforts** to keep the infrastructure and resources needed to execute and deliver it funded - **through the end of the Retrieval Period and the delivery of every export requested within it**, for every affected Customer.

AI-provider retention (disclosure). Aidealy uses two AI model providers for the AI features of the Service (analysis and scoring of source code, classification of developers' typed messages, and the natural-language analytics assistant): **OpenAI OpCo, LLC** and **Anthropic, PBC**. 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 that being a new or replacement Sub-processor (Section 6.2). Both providers' retention terms are therefore disclosed here, and each applies to whichever step is routed to that provider. **Where a step runs through OpenAI's batch and file interfaces**, Aidealy sends the requests with storage switched off, deletes the files it uploads and the files the batch produces once the results are persisted, and in any case sets each of those files to expire **forty-eight (48) hours** after the file is created; the batch record itself, which OpenAI's interface offers no way to delete, is a status record (identifiers, timestamps, the model used, request and token counts, tags and any validation-error messages) and holds none of the request or response content. OpenAI's published policy: its abuse-monitoring logs are kept for **up to 30 days** unless the law requires longer or retention is reasonably necessary to protect its services or a third party from harm; batch data and uploaded files persist as application state until deleted; neither endpoint is eligible for zero data retention; and, more generally, OpenAI may retain API inputs and outputs for **up to 30 days** to provide its services and to identify abuse, after which they are removed unless it is legally required to retain them. The corresponding disclosure for the analytics assistant's conversation store, where the assistant is routed to OpenAI (the "at least 30 days" floor), is set out above. **Where a step is routed to Anthropic**, Anthropic's published policy deletes API inputs and outputs **within 30 days** of receipt or generation, except for a service with longer retention under the customer's control, a zero-data-retention agreement, enforcement of its Usage Policy, and legal requirements; where a step runs through Anthropic's Message Batches API, that interface stores request and response data for **up to 29 days** after batch creation and is not eligible for Anthropic's zero-data-retention arrangements. These figures are the providers' published policies, **not deletion dates Aidealy promises**: each provider may retain content for substantially longer where its automated trust and safety systems flag it or where it considers retention reasonably necessary to protect its services or others from harm, and may retain data where required by law. Under their respective commercial terms, **neither provider trains its models on this content** (Section 2 of the AI Addendum and Section 4.3 of the Agreement).

11. International transfers

11.1 **Customer → Aidealy (Israel).** Aidealy is established in **Israel**, which benefits from a European Commission **adequacy decision** (Decision 2011/61/EU, reviewed and upheld on 15 January 2024) and from **UK adequacy**. Transfers of Customer Personal Data from the EEA or the UK to Aidealy in Israel therefore do not require an additional transfer safeguard.

11.2 **Adequacy fallback.** If the adequacy decision for Israel ceases to apply, the **SCCs (Module Two, controller-to-processor)** and, for UK data, the **UK Addendum** are deemed incorporated into this DPA and take effect for transfers from the EEA/UK to Aidealy, populated by Annexes I-III and by Annex IV.

11.3 **Aidealy → Sub-processors.** Where Aidealy transfers Customer Personal Data to a Sub-processor in a third country that does not benefit from adequacy, Aidealy relies on the **SCCs (Module Three, processor-to-processor)** and, for UK data, the **UK Addendum**, together with a transfer risk assessment. Aidealy does not rely on the EU-US Data Privacy Framework as the sole mechanism for any transfer. Annex IV maps the transfer for each Sub-processor.

11.4 **Israeli-law transfers.** For transfers from Aidealy's Israeli operations to Sub-processors abroad, Aidealy obtains from each Sub-processor, in the Sub-processor contracts and for the purposes of the Israeli Protection of Privacy (Transfer of Data Abroad) Regulations, undertakings to apply protections no less protective than those for a database in Israel, and not to transfer the data onward except to processors that the Sub-processor engages, that Aidealy has authorised in writing and that are bound by data-protection terms comparable to those the Sub-processor owes Aidealy. The Customer's general written authorisation in Section 6.1 also constitutes the Customer's written consent to those onward transfers; Aidealy conveys that consent to each Sub-processor, on the Customer's behalf, in the Sub-processor contracts.

11.5 **Direct collection.** Where a Data Subject provides Customer Personal Data directly into a region of the Service (for example, an EEA-resident user of a Customer tenant hosted in the United States), that direct collection is not by itself a restricted transfer; the transfer safeguards in this Section apply to onward disclosures by Aidealy to its Sub-processors. The **AI-model inference leg** is such an onward disclosure for **every** region (including the EU region): the content the AI features of the Service submit (source code for analysis and scoring, developers' typed messages for classification, and the analytics assistant's inputs) is disclosed to whichever of the two listed AI providers performs the step - **Anthropic, PBC**, a US-based processor with **no EU-resident option** (inference runs in US infrastructure for US tenants and may run in any geography for others, and Anthropic stores the API data in the **United States**), or **OpenAI OpCo, LLC** (processing at its default endpoint, its EU regional option being supported in Aidealy's software but not switched on) - and is covered by the Module 3 Standard Contractual Clauses in Annex IV.

12. Audits and information

12.1 **Demonstrating compliance.** Aidealy makes available to the Customer the information necessary to demonstrate compliance with this Section and with Art. 28, and allows for and contributes to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer.

12.2 **How audits are satisfied.** Because Aidealy is a cloud-based service that operates **no physical premises** of its own and hosts data with the infrastructure Sub-processors in Annex III, Aidealy satisfies this obligation primarily by providing: its third-party audit reports and certifications **once obtained** (see Annex II), responses to a reasonable security questionnaire, and written information describing its measures. An on-site or independent inspection is limited to where it is required by a Supervisory Authority or where the Customer has a reasonable, documented basis to believe Aidealy is in material breach; it takes place on reasonable prior notice, during business hours, no more than once in any 12-month period (except for-cause or as a regulator requires), subject to confidentiality, without access to other customers' data, and at the Customer's cost. On the Customer's reasonable request, Aidealy will also make available **summaries of its transfer risk assessments** for the transfers described in Section 11 and Annex IV, subject to the confidentiality obligations of the Agreement.

13. United States State Privacy Laws

13.1 **Service-provider / processor status.** To the extent Aidealy processes Personal Data subject to a US State Privacy Law, it acts as the Customer's **service provider / contractor** (CCPA) and

processor (other states), and the Customer is the **business / controller**. The Customer discloses Personal Data to Aidealy only for the **limited and specified business purposes** of providing the Service, set out in Annex I.

13.2 **Restrictions and certification.** Aidealy will not: **sell or share** the Personal Data; retain, use or disclose it for any purpose other than the specified business purposes, for any other commercial purpose, or outside the direct business relationship with the Customer; or combine it with Personal Data from other sources except as the CCPA permits. **Aidealy certifies that it understands these restrictions and will comply with them.**

13.3 **Same protection; sub-contracts; assistance.** Aidealy provides at least the same level of privacy protection as the CCPA requires, notifies the Customer of and binds any sub-processor by written contract to the same restrictions, notifies the Customer if it determines it can no longer meet its obligations, grants the Customer the right to take reasonable steps to stop and remediate unauthorised use, and enables the Customer to respond to consumer-rights requests. Taking into account the nature of the processing and the information available to it, Aidealy will also provide the Customer with reasonable assistance and information, insofar as it concerns Aidealy's processing of the Personal Data, to support the Customer's **cybersecurity audits**, **risk assessments**, and **automated decisionmaking technology** compliance obligations under the CCPA and its regulations.

14. Israeli Protection of Privacy Law

Where the Israeli PPL applies, Aidealy acts as a **"holder" (מחזיק)** processing the Customer's database on its behalf, and this DPA constitutes the written outsourcing instruction required by the Israeli Data Security Regulations: it sets out the data and permitted purposes, the systems accessed, the permitted processing, the duration and return/destruction of data, the security measures and applicable security level, personnel confidentiality, sub-processor flow-down, and Aidealy's reporting and security-event-notification duties. The applicable security level under the Israeli Data Security Regulations, on the classification criteria of their Schedules, is currently the lighter regime the Regulations set for a **database managed by an individual** and, once that regime no longer applies, the **basic level**; Aidealy **re-classifies the database as the classification facts change** - in particular when the number of data subjects reaches 10,000, when the number of authorised access holders grows, or if a First-Schedule data category enters the database - and applies the duties of the level then applicable.

Amendment 13 note. Under Amendment 13 to the Israeli PPL, assessment data about an individual's functioning at work can constitute **"specially sensitive information"**; Aidealy applies the duties that classification carries where it applies, and the parties' roles are unchanged by it.

15. Liability

The liability of each party under or in connection with this DPA is subject to the **limitations and exclusions of liability in the Agreement**. Nothing in this DPA limits either party's liability where it may not be limited under applicable law. As between the parties, each party's responsibility for damage caused by processing follows the allocation in Data Protection Law (a processor is liable where it has not complied with obligations directed specifically to processors, or has acted outside or contrary to the Controller's lawful instructions).

Regulatory fines and response costs. The allocation in **Section 12.5 of the Agreement** applies to administrative fines, monetary penalties, and regulatory-response costs arising from the processing of Customer Personal Data: each party bears them **to the extent attributable to the other party's breach of this DPA or the Agreement and legally indemnifiable**, with the fault carve-out, the read-down savings, and the response-costs limb stated there. For clarity, that allocation is **subject to the limitations and exclusions of liability in the Agreement**: the Agreement's uncapped-indemnity carve-out (its Section 11.3(d)) extends only to the defence and third-party indemnities in its Sections 12.1 and 12.2, so amounts allocated under Section 12.5 - including the response-costs limb - **count toward, and are limited by, the Agreement's aggregate liability cap**,

save where liability may not be limited under applicable law. That allocation includes the **notification-cost reimbursement in Section 12.5(b) of the Agreement** - Aidealy's reimbursement, where a Security Incident results from Aidealy's material breach of the Agreement (including this DPA), of the Customer's reasonable, documented costs of the notifications applicable law requires the Customer to make to authorities and to affected individuals - which is likewise **within, and limited by, the Agreement's aggregate liability cap** (its Section 11.2), as Section 12.5(b) itself states.

16. General

16.1 **Governing law.** This DPA is governed by the **law and jurisdiction of the Agreement** - currently the **laws of the State of Israel**, subject to the mandatory-rights savings clause in the Agreement - except that the EU SCCs are governed by the law of **Ireland** as stated in Annex IV.

16.2 **Order of precedence.** In case of conflict on the processing of Customer Personal Data: the SCCs (and UK Addendum), then this DPA, then the Agreement. For a Customer within the scope of the **EU Data Act Rider** (its Section 1.1), and solely for the subject matter that Rider addresses, the **timing rules of the Rider** (its notice period, transitional period, and the start of the Retrieval Period on a switching exit) apply **in place of the default timing in Section 10 of this DPA**, as the Rider's Sections 1.4 and 5 state; Section 10's export and erasure mechanics otherwise continue to apply, and nothing in this sentence affects the precedence of the SCCs (and UK Addendum) stated above.

16.3 **Records.** Each party maintains the records of processing required of it by Data Protection Law. Aidealy maintains its own processor record of processing activities.

16.4 **Changes.** Aidealy may update this DPA to reflect changes in Data Protection Law or guidance, in the Service, or in Aidealy's Sub-processors, operations or measures. A new version of this DPA takes effect for the Customer as the Agreement's "Changes to this Agreement; version binding; records" provision states: a version that materially reduces the protections for Customer Personal Data takes effect at the start of the Customer's next renewal term, on reasonable notice, and any other version takes effect as that provision states for other changes. The version of this DPA in effect for a subscription term is the Customer's documented instruction under Section 3.1 for that term, including for Customer Personal Data collected under an earlier version. Nothing in this Section varies the Standard Contractual Clauses or the UK Addendum, or permits a change that the Agreement states cannot be made by an update (its Section 4.3).

16.5 **No third-party beneficiaries, except as data-protection law provides.** This DPA is for the benefit of the parties and **creates no right enforceable by any person who is not a party, except that**: (a) **Data Subjects may invoke and enforce the Standard Contractual Clauses as third-party beneficiaries as, and to the extent, the SCCs themselves provide** (Clause 3 of the SCCs referenced in Section 11 and Annex IV), and nothing in this DPA limits or modifies those rights; and (b) nothing in this DPA limits any right a Data Subject or any other person has **under Data Protection Law or other applicable law** (including a Data Subject's rights and remedies against Controller or Processor under the GDPR). Subject to those exceptions, only the parties may enforce this DPA.

16.6 **Assignment; successors.** This DPA **follows the Agreement**: it may not be assigned separately from the Agreement, and a permitted assignment of the Agreement (under its Assignment provision, Section 15 of the Agreement) assigns this DPA with it, without further consent. This DPA **binds and benefits the parties and their respective permitted successors and assigns**, and a successor to a party under a permitted assignment assumes that party's rights and obligations under this DPA (including, for Aidealy, the processing commitments and the SCCs' obligations for transfers it continues to make).

Annex I - Details of the Processing

A. Parties.

Role	Party
Controller / business	The Customer identified in the Agreement (and, where the Customer is itself a processor, the underlying controller).
Processor / service provider / holder	Aidealy Ltd., Hamidron 1, Herzliya 4654110, Israel - privacy@aidealy.ai.

B. Subject-matter and duration. Aidealy's processing of Customer Personal Data to provide the Service, for the term of the Agreement plus the return/deletion period in Section 10.

C. Nature and purpose of the processing. Hosting, storage, analysis and processing of the Customer's software development data to provide Aidealy's code-quality and developer-activity analytics and its AI analytics features - including transmitting source code to AI sub-processors for automated scoring, storing code/diff content and IDE/AI-assistant interaction data, and computing team- and developer-level metrics (for each developer: an estimate of the time actively spent on their changes, or "effort hours", in two variants; the volume of code they contributed and its split between AI-assisted and human-written; and the AI-model token usage attributable to them), and classifying the text of developer prompts (the part of the system the message is about, the kind of work being asked for, any quality concern raised, and the apparent tone) to compute work-pattern and per-developer experience metrics - solely for the **limited and specified business purpose** of providing, securing, maintaining and supporting the Service for the Customer. The effort-hours metric is computed from **IDE and git activity signals only**: it does not and cannot measure an individual's overall working time, presence, meetings, or any work performed outside those signals, and the Customer must not use it as a measure of an individual's total working time, presence, or inactivity, and must not use it as a criterion for determining an individual's pay, bonuses, or pay progression (AI Addendum Section 5.6).

Temporal scope of the processing - historical backfill. The historical backfill of the git repositories the Customer selects loads, and Aidealy processes, repository and development history from within the **Backfill Window** stated in the Order Form. That bound is applied to every repository the Customer selects and to every git provider the Service supports as at the date the then-current version of the Agreement was published by Aidealy, subject to the exceptions below. As one of those exceptions, the Service may read a temporary copy of a selected repository's whole history to compute its results; it stores nothing it reads there about history predating the Backfill Window, and deletes the copy afterwards. Whether history falls within the Backfill Window is determined by the **dates the git provider records** for that history, which may differ from when the work was originally performed where history has been rewritten (for example on rebase, squash, or import). **Pull-request closing times.** Where a git provider does not make available the time at which a pull request (or equivalent merge request) was closed or merged, the Service treats the time of that pull request's most recent activity recorded by that provider as its closing time. On such a provider this affects **every** pull request that was declined or superseded rather than merged, and it may also affect merged ones; a pull request whose activity had ended before the Backfill Window but which was commented on or otherwise touched within it **will be loaded**. Where a pull request is loaded in that way, that pull request's **own** records are loaded whatever their date, including the whole of its review and discussion thread and the **username, display name and email address** the git provider records for each person who took part in it - a population that includes individuals outside the Customer's organisation (Annex I.E). **No other pull request, and no other repository history, is loaded by reason of this exception**, and **commit history is not affected**: commit ingestion is separately bounded by commit date. Aidealy identifies the affected git providers in the **Documentation**. **The IDE extension's upload and the Claude Code collector's one-time history upload are separate and are not bounded by the Backfill Window** - see the "Backfill upload staging" paragraph of Section 10; each remains a "historical backfill" for the purposes of Section

3.2 of this DPA and Section 4.2(c) of the AUP. *(Agreement Section 1, "Backfill Window", and Section 2.10; AUP Section 4.2A(c).)*

Repository scope of the processing. The Service processes only records from repositories within the Customer's **connected git accounts** and selected **analysis scope** (each as defined in Section 1 of the Agreement), as the Agreement provides (Section 4.1 of the Agreement). When a record received from the Aidealy client software on an individual's machine (the IDE extension or the Claude Code collector) is processed, the Service checks the repository it came from against that scope. A record from any other repository - including a personal project of the individual, a repository the Customer has not connected, a working folder that is not a repository or has no remote address, or a repository the Customer has excluded - is discarded when it is processed and is not stored: nothing about it is analysed, and only counts of the discarded records and the reasons for discarding them are kept, never the repository's name or address. The one exception on that path is each upload of the history held on the machine itself (the IDE extension's database copy, uploaded on first set-up and again in the cases stated in the "Backfill upload staging" paragraph of Section 10, and the Claude Code collector's one-time history archive), which arrives as a single file before any record in it is read and sits in the upload staging store, unfiltered, until it is processed and erased or expires under the "Backfill upload staging" paragraph of Section 10. Each history upload carries a map of the repositories it refers to, built on the individual's machine, and is gated by the same rule; for the IDE extension's database copy the verdict is taken per session, from the repositories that session's own code changes belong to, and a session with no code changes is discarded. A record that touches more than one repository is kept where any one of them is within scope. The Claude Code collector's own session, workspace and commit records are kept whatever project they came from: they carry no repository address or account name (nothing the scope rule can match), but they do carry the name of the working folder (the last segment of its path, which is often the name of the repository's directory), a folder identifier derived from the full path, the session's start and end, and, for a commit record, the commit identifier, the kind of operation and the counts of files and lines changed. The verdict is taken when the record is processed and is not revisited if the Customer later changes its connected git accounts or analysis scope; where the scope cannot be established when a batch is processed, the batch is not accepted and the client software sends it again later, so that no record is stored on an unknown verdict. **A Customer that has connected no git account receives no repository content from any developer's machine**: every record from a repository is discarded until a git account is connected, and only the Claude Code collector's session, workspace and commit records described above (folder name, folder identifier, session times and per-commit identifiers and change counts, never file content, prompts or responses) are kept. The upload itself is still used to identify the individual and the Customer's account.

D. Types of Customer Personal Data.

Category	Examples
Source code and repository content	File contents, diffs/hunks, and any personal data the Customer's code contains
Pull-request records	Pull-request titles and descriptions; the individuals recorded as opening, reviewing, or merging a pull request; and the review and discussion thread - including the username, display name and email address the git provider records for each participant
Git identity	Author / committer names and email addresses
IDE / AI-assistant interaction data	Prompts, responses and code context from the Aidealy client software on the individual's machine: from the IDE extension (Cursor), the text of the individual's AI chat and

Category	Examples
	agent sessions and the code differences Cursor records; from the Claude Code collector, the full session transcripts Claude Code writes, uploaded as written and without a content filter - every prompt the individual types and every model response, the full text of the files the tool read and the changes it wrote, the output of the commands it ran (verbatim), the images and documents the individual pasted into a conversation (including any third-party content in them), the code differences the individual's working files received, and the repository, branch and commit context - collected from every project the individual uses Claude Code in, personal projects included, subject to the repository-scope rule in Part C
Developer account identifiers	IDE/assistant user id and email; for the Claude Code collector, the individual's email address and account and organisation identifiers read from the machine's Claude Code sign-in (or from an IT-managed settings file or a cloud sign-in), the **git email address configured in each repository the individual works in** (used only to match the individual to a person the Customer's account already knows; it never creates a new user record), the individual's account name on the code host, and a random installation identifier. Where the Customer uses automatic provisioning and the individual's email domain is one the Customer has verified, a user record and a seat are created for the individual on the first accepted upload, without administrator action
Developer-activity metrics	Activity and contribution metrics computed per developer - including estimated active-work time/effort computed from IDE and git activity signals only (in two variants; not a measure of overall working time or presence), code volume, the split between AI-assisted and human-written code, and attributable AI-model token usage
Message classification	Automated labels for each prompt the individual types into the IDE extension's AI chat or into Claude Code - the part of the system the message is about, the kind of work being asked for, any quality concern raised, and the apparent tone - derived from the message **text** only, read together with up to three of the individual's previous messages in the same session

Aidealy does not seek special-category (Art. 9) or criminal-offence (Art. 10) data; the Customer must not submit it without prior agreement (Section 3.4).

E. Categories of Data Subjects. The Customer's developers and other personnel whose code, commits, identity or development activity is processed through the Service; **individuals outside the Customer's organisation who contributed to, reviewed, or commented on the repositories the Customer selects - for example external and open-source contributors - and whose git identity or pull-request participation the git provider records**; and any individuals identifiable within the Customer's source code, commit history, pull-request records or AI-assistant interactions. *(The Customer's transparency duties to the second class are addressed in Section 4.2(d) of the AUP.)*

F. Frequency. Continuous, for the duration of the Customer's use of the Service.

G. Competent supervisory authority. Where the SCCs apply, the competent supervisory authority is determined in accordance with **Clause 13 of the SCCs**: **(i)** where the Customer is established in an EU Member State, the supervisory authority of that Member State; **(ii)** where the Customer is not established in an EU Member State but falls within the territorial scope of the GDPR under Article 3(2) and has appointed a representative under Article 27, the supervisory authority of the Member State in which the representative is established; and **(iii)** where the Customer falls within Article 3(2) but is not required to appoint a representative under Article 27(2), the supervisory authority of one of the Member States in which the Data Subjects whose personal data is transferred are located. The specific authority for a given Customer follows from the Customer's establishment (or representative) as identified in the Agreement or the applicable Order Form. For transfers subject to the UK GDPR, the competent authority is the UK Information Commissioner's Office or its successor, the Information Commission.

Annex II - Technical and Organisational Measures

Aidealy maintains the following measures (GDPR Art. 32).

Area	Measure
Encryption	Encryption of Customer Personal Data **stored in the Service** using per-tenant managed encryption keys; **TLS** in transit.
Tenant isolation	Logical isolation per customer: row-level security, a tenant identifier enforced in access tokens, per-tenant database (enterprise), and per-tenant encryption keys.
Access control & authentication	Authentication via password with optional two-factor (TOTP), email magic-link, Google sign-in, and SAML single sign-on; least-privilege access for personnel.
Developer-tool access (IDE extension)	The IDE extension identifies users by reusing the developer's existing editor sign-in; extension telemetry is accepted only for users matched to the Customer's account, through an email address under a Customer-verified domain or, otherwise, an address a Customer administrator has added to the account and approved; Customer administrators can require per-user approval before ingestion; and each editor sign-in account is bound to the first user it is seen for in the Customer's organisation, a control designed so that a different user in the Customer's organisation presenting that account is refused.
Data-region segregation	Strict separation of the EU (eu-west-1) and US (us-east-1) regions; each customer tenant is pinned to one region with no transfer of data between regions.
Logging & monitoring	Recording of account-security events (e.g. sign-in, two-factor checks, single-sign-on enforcement, tenant switch) and application error monitoring.

Area	Measure
Confidentiality & personnel security	Aidealy is currently **founder-operated**: production access is confined to the founder, under least-privilege access controls, logging, and multi-factor authentication. For **any personnel Aidealy engages, the following apply as commitments from the first hire**: binding confidentiality obligations; personnel screening where, and to the extent, applicable employment law permits; security-awareness training on an annual cadence; and periodic access reviews. Processing only on instructions.
Resilience & recovery	Backups and the ability to restore availability of Customer Personal Data.
Vulnerability management	Automated dependency and code scanning (continuous CVE/OSV scanning, static code analysis, and secret scanning gating merges to the main branch); internal remediation **targets** by severity - **7 days (critical), 30 days (high), 90 days (medium), 180 days (low)** - stated as Aidealy's internal targets, not a measured track record; a published Vulnerability Disclosure Policy with a coordinated-disclosure channel.
Secure development	Peer review of code changes before merge (an automated multi-reviewer gate with mandatory conversation resolution on protected main branches) and continuous-integration security checks.
Incident response	A documented incident-response runbook; an internal register of security incidents (retained five years); the notification commitments in Section 9 and the Breach-Notification Commitment.
Physical security	Physical and environmental security of the hosting infrastructure is provided by the cloud providers (AWS, Vercel) under their own audited compliance programmes; Aidealy operates no data centre of its own.
Pseudonymisation & data-subject support	Per-individual de-identification of identity records (Section 10); hash-only storage of code-diff content; content-storage gating that keeps raw prompt/response text out of the production analytics stores at rest (the upstream exceptions being a typed prompt, which waits in our systems until it has been classified and is then deleted, normally within a few hours, and the upload staging copy described in Section 10, erased on successful processing and in any case expiring after about eight (8) days); the Data-Subject-rights assistance measures in Section 7.

Area	Measure
Business continuity / disaster recovery	Aidealy maintains **commercially reasonable disaster-avoidance procedures** designed to safeguard Customer Data and the Service's availability, including **backups taken at least daily** with restore capability (see Resilience & recovery); a **formal business-continuity and disaster-recovery plan with stated recovery objectives is on Aidealy's roadmap and is not yet in place** - recovery-time and recovery-point objectives will be added to this Annex when they exist.
Governance	**SOC 2 and ISO/IEC 27001 are planned and not yet certified**: Aidealy targets a **SOC 2 Type I report within twelve (12) months of the Service's general availability, with ISO/IEC 27001 to follow** - a target Aidealy pursues in good faith, not a warranty or a promised certification date. Aidealy will make any report or certificate available once obtained; this Annex describes Aidealy's current controls and roadmap and does **not** represent a current certification.

Government requests. Aidealy's commitments on government and law-enforcement requests for Customer Personal Data are set out in Section 3.5.

Annex III - Authorised Sub-processors

Sub-processors of **Customer Personal Data** as at the date of this DPA.

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

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

*Notes: the two AI model providers, **Anthropic, PBC** and **OpenAI OpCo, LLC**, are each authorised for all the AI features of the Service (analysis and scoring of source code, classification of developers' typed messages, and the natural-language analytics assistant): either may perform any of those steps, and Aidealy chooses the routing and may change it at any time, including as a fallback when one provider is unavailable, without that being a new or replacement Sub-processor (Section 6.2); the "AI-provider retention" paragraph of Section 10 discloses both providers' retention terms. **AWS Bedrock AgentCore Code Interpreter** is a service of Amazon Web Services, not a further Sub-processor: the analytics assistant's generated analysis code runs in an isolated sandbox session that Aidealy opens in the Customer's own data region. **LangSmith (LangChain)** is listed on a forward basis: its tracing integration is wired in the shipped production library but*

***dormant** - no LangSmith API key is provisioned and **no Customer Personal Data flows to LangChain until it is**; activation is conditioned on the LangChain DPA being executed and on file first (Section 6). **Contracting entities**: for EEA/EMEA the Amazon entity is **Amazon Web Services EMEA SARL** (Luxembourg) and OpenAI's contracting entity is determined by the customer's location under OpenAI's Services Agreement (**OpenAI OpCo, LLC** for a customer outside the EEA and Switzerland, which is Aidealy's case); ArangoDB is contracted through **ArangoDB GmbH** (Germany). **LangSmith is not region-separated**: the shipped wiring uses LangChain's default United-States endpoint (no EU data-residency pinning), so tracing data - once the integration is activated - is processed in the United States under the Annex IV SCC mechanism. **Anthropic** has **no EU data-residency option** on its first-party API: for all regions, the content of any AI step routed to it is disclosed to a US-based processor and **stored by Anthropic in the United States** (inference runs in US infrastructure for US tenants and may run in any geography for others - no region guarantee) - the request content only, held under the retention terms in Section 10 and not used to train models; the transfer is covered by Annex IV. **OpenAI** data residency is set per project (or per request from a global project) and requires OpenAI's EU regional endpoint (`eu.api.openai.com`). Aidealy's library supports that regional routing, but it is **wired behind a feature flag that is OFF by default and not yet enabled**, so **today OpenAI processing runs at the default endpoint** (covered by the Annex IV SCCs). EU-resident OpenAI processing becomes available only once the operator completes the OpenAI account prerequisites (OpenAI's approval for Modified Abuse Monitoring or Zero Data Retention, and a Modified Retention amendment for a region outside the United States) and enables the flag; the `/v1/conversations` object that holds the analytics assistant's server-side conversation state, where the assistant is routed to OpenAI, is a standing carve-out that OpenAI does not list as a residency-covered endpoint.*

Annex IV - Cross-Border Transfer Mechanisms

Governing law / forum of the SCCs: Ireland (SCC Clause 17, Option 1); courts of Ireland (Clause 18). **Docking (Clause 7):** applies. **Sub-processors (Clause 9):** Option 2 (general written authorisation), list in Annex III, kept up to date; advance notice per Section 6.2. The SCC Appendix is completed by **Annex I** (parties and description of processing), **Annex II** (technical and organisational measures) and **Annex III** (sub-processors).

Transfer map.

Transfer	Mechanism (current)	Notes
EEA Customer → Aidealy (Israel)	EU adequacy (Decision 2011/61/EU)	SCC Module 2 fallback if adequacy ends (§11.2)
UK Customer → Aidealy (Israel)	UK adequacy	IDTA / SCCs + UK Addendum fallback
Aidealy → Anthropic, PBC (US)	EU SCCs Module 3 + UK Addendum + transfer risk assessment	**Not DPF-certified** - SCCs are the mechanism (Module Three, incorporated in Anthropic's DPA together with the UK Addendum); covers any AI step routed to Anthropic; **no EU-resident first-party option** (Anthropic stores API data in the US for all regions; inference runs in the US for US tenants, any geography for others - no region guarantee)

Transfer	Mechanism (current)	Notes
Aidealy → OpenAI OpCo, LLC (US)	EU SCCs Module 3 + UK Addendum + transfer risk assessment	**Not DPF-certified** - SCCs are the mechanism (OpenAI's Data Processing Addendum incorporates the EU Standard Contractual Clauses, Module Three, and the UK Addendum); covers any AI step routed to OpenAI; EU-resident processing (`eu.api.openai.com`) is supported in Aidealy's software but is not switched on (a deployment flag, default OFF), so today processing is at the default endpoint under these SCCs; OpenAI's approval for Modified Abuse Monitoring or Zero Data Retention, a Modified Retention amendment, project (or per-request) residency and the operator flag flip are all required for an EU leg
Aidealy → AWS (US)	EU SCCs (+ DPF as supplementary) + transfer risk assessment	DPF-certified; EU data hosted in eu-west-1
Aidealy → Sentry (US)	EU SCCs (+ DPF as supplementary) + transfer risk assessment	DPF-certified
Aidealy → Vercel (US)	EU SCCs (+ DPF as supplementary) + UK Addendum	DPF-certified; EU front-end hosted in eu-west-1
Aidealy → Supabase / ArangoDB	EU SCCs (+ UK Addendum) in their DPAs	EU-hosted for EU tenants; covers their onward US sub-processing
Aidealy → LangChain, Inc. (LangSmith) (US)	EU SCCs (+ UK Addendum) in LangChain DPA + transfer risk assessment	Integration wired but dormant (no data flow today); LangChain DPA is request-based - execute it BEFORE the API key is provisioned and the flow activates; US endpoint, no EU pinning
Aidealy (Israel) → any Sub-processor abroad	Israeli Transfer Regs Reg 2(4) undertaking + Reg 3 guarantee	Carried by the Sub-processor contracts (§11.4)

The EU-US Data Privacy Framework is treated as a supplementary protection only, never as the sole transfer mechanism, and the transfer risk assessments take account of the legal developments bearing on it.

Annex V - Additional Jurisdiction Provisions (Korea, Japan, UAE)

Purpose and effect. This Annex explains how the commitments in the body of this DPA satisfy the processor-contract requirements of the Republic of Korea, Japan, and the United Arab Emirates, for Customers whose processing is subject to those laws. It is a **mapping and clarification of the body of this DPA**: except for the two sentences expressly identified below (the Korean cooperation sentence in Part A and the UAE processing-record sentence in Part C), this Annex creates **no obligations beyond those in the body of this DPA**, and if this Annex conflicts with the body of this DPA, **the body of this DPA prevails - save that those two expressly identified sentences are operative obligations of Aidealy and take effect in addition to the body of this DPA**. This Annex is part of this DPA for the purposes of Section 16.2. Capitalised terms have the meanings given in this DPA.

A. Republic of Korea - Personal Information Protection Act (PIPA).

Outsourcing document and mandatory content. For a Customer subject to PIPA, this DPA is the written outsourcing document required by Article 26(1) of PIPA, and the content made mandatory by Article 26(1) of PIPA and Article 28(1) of its Enforcement Decree is located in this DPA as follows:

Mandatory content (PIPA Art. 26(1); Decree Art. 28(1))	Where in this DPA
Prohibition of processing beyond the purpose of the entrusted work	Sections 2 and 3.1; Annex I (part C)
Technical and managerial safeguards for the personal information	Section 5.1; Annex II
Purpose and scope of the entrusted work	Section 2; Annex I (parts B to F)
Restriction on re-entrustment	Section 6 (Sections 6.1 to 6.3); see "Re-entrustment" below
Safety measures, including restriction of access to the personal information	Section 5.1; Annex II (access-control and tenant-isolation rows)
Supervision, including inspection of the management status of the information	Sections 12.1 and 12.2 (including the for-cause inspection route); 6.4
Liability, including damages, for a breach of the trustee's duties	Section 15; Section 6.3 (full liability for Sub-processors)

Re-entrustment (Article 26(6)). For the purposes of Article 26(6) of the Korean Personal Information Protection Act, the Customer's general written authorisation in Section 6.1, together with the Annex III list and the notice-and-objection mechanism in Sections 6.2 and 6.2A, constitutes the Customer's prior written consent to each re-entrustment of the processing described in this DPA, and Aidealy will not permit any re-entrustment to which the Customer has objected under Section 6.2. Article 26(6) prescribes no form and no per-entity granularity for that consent; should a Korean Customer or the Personal Information Protection Commission take the stricter reading that Article 26(6) requires consent for each re-entrustment individually, the Section 6.2 notice window already functions as an individual, advance consent request for each change (consent standing by non-objection after individual notice), and an objection under Section 6.2 withholds that consent.

Supervision and education (Article 26(4)). Aidealy will reasonably cooperate with the Customer's duty under Article 26(4) of PIPA to educate its trustee and to supervise the trustee's safe processing of the personal information, including through the audit, inspection and information rights in Section 12 and the diligence information in Section 6.4.

Overseas entrustment (Article 28-8). A Korean Customer's entrustment of processing to Aidealy in Israel is also an overseas transfer of personal information under Article 28-8 of PIPA. Article

28-8(1)3 of PIPA provides a route for that transfer without data-subject consent where the overseas processing-entrustment or storage is necessary for the conclusion and performance of the contract with the data subject and the items listed in Article 28-8(2) are disclosed in the Customer's privacy policy under Article 30 or notified to the data subjects. Most of the information the Customer needs for that disclosure is set out in this DPA: the items of personal information transferred (Annex I, part D); the destination country (Israel) and the recipient's identity and contact details (the preamble and Annex I, part A); the time and method of the transfer (continuous transmission through the Service for the duration of the Customer's use, Annex I, part F, over encrypted connections, Annex II); the purpose and retention periods (Annex I and Section 10); and the onward recipients and safeguards (Annexes III and IV and Section 11). The method and procedure by which a data subject may refuse the overseas transfer, and the effect of a refusal, depend on the Customer's own processes and are for the Customer to state in its privacy policy or notice; Aidealy will provide, on request, the further information the Customer reasonably needs for its Article 28-8(2) disclosure. The Customer remains responsible for selecting, and satisfying the conditions of, its Article 28-8 transfer route.

B. Japan - Act on the Protection of Personal Information (APPI).

Supervision of the trustee (Article 25). A Japanese Customer entrusting the handling of personal data to Aidealy must exercise necessary and appropriate supervision over Aidealy under Article 25 of the APPI. The audit and information rights in Sections 12.1 and 12.2, the diligence information in Section 6.4, the security measures in Section 5 and Annex II, and the breach notification in Section 9 are the contractual means through which the Customer exercises that supervision. For the entrustment itself, a trustee is not a "third party" for the purposes of Article 27 of the APPI (Article 27(5)(i)).

Provision to a third party in a foreign country (Article 28). Aidealy is established in Israel, which, as at the date of this DPA, is not among the countries designated under Article 28(1) of the APPI and Article 15 of the PPC Enforcement Rules as having an equivalent protection regime (that designation covers the EU member states and the United Kingdom). A Japanese Customer's entrustment to Aidealy therefore proceeds on the basis that Aidealy, as the recipient, has in place a system conforming to Article 16 of the PPC Enforcement Rules for continuously implementing measures equivalent to the obligations of Chapter IV, Section 2 of the APPI (equivalent measures), unless the Customer instead obtains the data subject's consent. The parties intend and agree that **this DPA constitutes the "appropriate and reasonable method" under Article 16(i) of the PPC Enforcement Rules by which the implementation of those equivalent measures is ensured**: the obligations in Sections 3 to 12 of this DPA (documented instructions, confidentiality, security, Sub-processor flow-down, assistance, breach notification, return and deletion, and audits) correspond to that duty set.

Ongoing confirmation and information to data subjects (Article 28(3); Rules Article 18). Through the information and audit rights in Section 12, the Sub-processor change notices in Section 6.2, and the breach information in Section 9, Aidealy will provide the information the Customer reasonably needs to periodically confirm Aidealy's implementation of the equivalent measures and the relevant legal developments in the countries where the data is handled (Rules Article 18), and to inform data subjects, on request, about Aidealy's implementation of those measures (Article 28(3)).

C. United Arab Emirates - Federal Decree-Law No. 45 of 2021 (PDPL).

Appointment and processor obligations (Articles 7 to 9). This DPA, together with Annex II, provides the sufficient guarantees of technical and organisational measures that Article 7(5) of the PDPL requires a controller to obtain when appointing a processor. The processor obligations and mandatory contract content of Articles 8 and 9(3) of the PDPL are located in this DPA as follows:

PDPL provision	Requirement	Where in this DPA
Art. 8(1)	Processing per the controller's instructions and a contract specifying the scope, subject, purpose, nature and type of personal data and the categories of data subjects	Sections 2 and 3.1; Annex I
Art. 8(2)	Technical and organisational measures, including at the design stage	Sections 5.1 and 5.2; Annex II
Art. 8(3)	Processing within the specified purpose and period; the controller's authorisation for any extension	Section 3.1; Annex I (part B, duration)
Art. 8(4)	Erasure or return of the data after the processing period	Section 10
Art. 8(5)	No unauthorised disclosure	Section 4; Section 3.5
Art. 8(6)	Secure processing, media and devices	Section 5; Annex II
Art. 8(7)	Record of processing, produced to the competent authority on request	Section 16.3; "Processing record" below
Art. 8(8)	Proof of compliance on the controller's or the authority's request	Sections 12.1 and 12.2
Art. 8(10)	Written contracts clearly defining obligations, responsibilities and roles where several processors participate	Section 6.3
Art. 9(3)	Notice of a personal-data breach to the controller as soon as the processor becomes aware	Sections 9.1 and 9.5

For Article 9(3), the Section 9.1 commitment to notify **without undue delay after becoming aware** gives effect to the "as soon as it becomes aware" standard; the 72-hour figure in Section 9.1 is an outer bound, not a period Aidealy waits out.

Processing record (Article 8(7)). Aidealy maintains its own record of processing activities (Section 16.3), covering the particulars of its processing under this DPA, and will make that record available to the competent UAE data protection authority (the Bureau referred to in the PDPL) on a lawful request, where legally required.

Cross-border transfers; Executive Regulations (Articles 22, 23 and 28). As at the date of this DPA, the Executive Regulations contemplated by Article 28 of the PDPL have not yet been issued, and no adequacy list under Article 22 exists. Pending their issue, the parties treat the contractual safeguards in Section 11 and Annex IV of this DPA - including the incorporated Standard Contractual Clauses protections - as a contract imposing measures at the level of protection the PDPL requires, in the manner contemplated by Article 23(1) of the PDPL for transfers in the absence of an adequacy decision. Aidealy will revisit this Annex when the Executive Regulations are issued.