graine.ai

GRAINE TRUST CENTER · DOCUMENT

Data Processing Agreement: summary

GR-PUB-15 · Version 1.2

Approved — effective 3 November 2026

DOCUMENT ID	VERSION	CLASSIFICATION
GR-PUB-15	1.2	Public

Document control

DOCUMENT ID	GR-PUB-15
VERSION	1.2
STATUS	Approved
OWNER	Privacy & Grievance Officer
APPROVED BY	Rishabh Bhanot, Founder (top management), 3 Nov 2026
EFFECTIVE DATE	3 Nov 2026
LAST UPDATED	4 Nov 2026
NEXT REVIEW	By 3 Nov 2027 (12 months after approval), or on a significant change
CLASSIFICATION	Public
APPLIES TO	Graine's data processing agreement with customers, for personal data Graine processes for them through the Graine AI platform

Contents

1. In short
2. What the draft provides
3. EU and UK rider
4. How to ask for the full DPA
Related documents
Revision history

1. In short

This is a plain-English summary of what Graine's data processing agreement (DPA) provides. It is not the agreement. **The full text is a draft that Graine is finalising, and it is not public.** Graine shares it with customers in contract once counsel has approved it. Where this summary and the signed agreement differ, the agreement governs. Statements are true as of 3 Nov 2026.

2. What the draft provides

TOPIC	WHAT IT SAYS
Roles	For the people a customer's agents contact, the customer decides why their data is used (the Data Fiduciary, or controller) and Graine is its Data Processor. For its own account and billing data Graine is a Data Fiduciary; the Privacy Notice covers that. The DPA is the contract section 8(2) of the DPDP Act requires, with the safeguards provision of Rule 6(1)(f).
Instructions only	Graine processes customer personal data only on the customer's documented instructions: the agreements, the platform settings it makes, and the calls its systems make through the API and SDKs. Graine says so if it thinks an instruction would break the law.
The customer's duties	The customer has a lawful basis, gives notices, obtains consent (including for recordings), follows telecom rules, discloses AI use where the law requires, obtains a parent's verifiable consent for children, keeps credentials secret, turns on the app and user protections before live end users, and reviews agent outputs.
Security	Reasonable security safeguards, set out in an annexure that separates what is in place from what is Being rolled out. Graine will not materially weaken the protections in place during the term, and reviews them yearly and after any breach.
Staff	Everyone Graine authorises to process customer personal data is bound by confidentiality, by contract or by law. Confidentiality agreements and security training for everyone with access are Planned; none has started.
Sub-processors	Graine gives 30 days' notice before adding or replacing a sub-processor on its public list or changing a region. The customer may object on reasonable data-protection grounds; the agreement says what happens if the parties cannot agree. Graine stays responsible for its sub-processors. Most vendors include data processing terms in the terms Graine accepted; Graine's copies are not yet on file, and filing them is Planned.
Locations	Only where the list shows. Call records and agents are in India (Mumbai); recordings are in the United Kingdom, a transfer outside India for Indian data; some model, speech, memory and knowledge-base providers process outside India. The customer authorises these transfers, which section 16 of the DPDP Act allows except to countries the Government restricts (Rule 15). If one is restricted, the parties agree how to meet it, for example a dedicated instance. The shared cloud does not pin a region for one customer.
Breach	Graine tells the customer of a breach affecting its data within 24 hours of confirming it, and updates it at least every 24 hours while the incident is open. The customer, as Data Fiduciary, tells affected people (Rule 7(1)) and the Data Protection Board without delay, with detail within 72 hours (Rule 7(2)); Graine gives it what it needs.

TOPIC	WHAT IT SAYS
Help	Graine helps the customer meet its duties to people under sections 11 to 14 of the DPDP Act and Rule 14. These cover access, correction, erasure, nomination and grievances. Graine also helps with impact assessments and regulators' enquiries. A request a person sends to Graine goes to the customer. Tools that find, export, correct and erase one person's data have been In place since 4 Nov 2026. They do not erase the copy of a call kept in a separate working store.
No training on customer data	Graine does not use customer data to train or fine-tune AI models. A custom voice is made only from recordings the customer gives for it. AI and speech vendors' use of data sent to them is set by their own terms; several use content to improve their models by default, and Graine is opting out wherever a vendor allows it.
Return and deletion	When the agreement ends, Graine returns the data on request and deletes it from live systems within 30 days of the customer's written instruction. It confirms deletion in writing on request. The copy of each call kept in a separate working store is not deleted by this. Backups age out on the providers' cycle; monthly database snapshots are kept 12 months.
One-year minimum	From 13 May 2027, where Rule 8(3) applies to the customer, personal data, traffic data and processing logs are kept at least one year from the date of processing, even after an erasure request or the end of the agreement. Graine keeps what the customer instructs, sealed from ordinary use, and deletes it when the year ends. The record this needs is Being rolled out.
Audit and information	Graine provides the annexure, a yearly questionnaire and a technical review with its engineers, and cooperates with a reasonable audit by the customer or its auditor, on notice. SOC 2 Type I: in progress. No SOC 2 report is held. ISO/IEC 27001:2022: in progress. No certificate is held. No independent penetration test has been done; one is planned.
Sensitive content	Health-related content may occur. The customer decides what its agents ask for; the platform does not filter content unless redaction is on. Memory is off until switched on, and then keeps names and health-related facts by default. The platform is not a medical device. HIPAA is not offered, and no business associate agreement is offered.
Order of documents	On data protection matters the DPA prevails over the main agreement. Liability, governing law and notices follow the main agreement and are not summarised here.

3. EU and UK rider

Where the GDPR or UK GDPR applies, a rider adds the terms of GDPR Art. 28(3): instructions, confidentiality, security, sub-processors, help with rights and assessments, deletion or return, and audit. India has no EU adequacy decision, so the rider incorporates the 2021 EU Standard Contractual Clauses, Module Two (controller to processor) or Module Three (processor to processor), and the UK International Data Transfer Addendum or Agreement for UK data. Graine's 24-hour breach notice meets "without undue delay" under Art. 33(2) and supports the controller's 72-hour duty to its supervisory authority under Art. 33(1). Health data is special-category data, so the customer needs an Art. 9 condition for it.

4. How to ask for the full DPA

Write to founders@graine.ai or use the request form at www.graine.ai/trust. Say who the contracting company is, whether EU or UK personal data is involved, and whether you also need a security questionnaire or a call with the engineers. Graine sends the agreement once counsel has approved it.

Related documents

- Privacy Notice
- Sub-processor List
- Security Overview
- Shared Responsibility Matrix
- Grievance Redressal Policy

Revision history

VERSION	DATE	CHANGE	APPROVED BY
1.0	2026-11-03	First issue, approved	Rishabh Bhanot, Founder
1.1	2026-11-04	Recordings' storage location corrected: the United Kingdom (Wasabi eu-west-3), not France; vendor training defaults stated; vendors' processor terms stated (in their terms or offered; Graine's copy not yet on file)	Correction; the approval of 3 Nov 2026 stands
1.2	2026-11-04	What erasure, retention and offboarding do not reach stated; data-request tools in place since 4 Nov 2026	Status update; the approval of 3 Nov 2026 stands