graine.ai

GRAINE TRUST CENTER · DOCUMENT

Shared Responsibility Matrix

GR-PUB-06 · Version 1.3

Approved — effective 3 November 2026

DOCUMENT ID	VERSION	CLASSIFICATION
GR-PUB-06	1.3	Public

GRAINE AI · MAVRIX AI PRIVATE LIMITED

Document control

DOCUMENT ID	GR-PUB-06
VERSION	1.3
STATUS	Approved
OWNER	Information Security Lead
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	The Graine AI business platform in its four deployment models: shared cloud, dedicated instance, your cloud account, and your own premises

Contents

1. In short
2. The four deployment models
3. The matrix
4. Customer-side controls
5. Contact
Related documents
Revision history

1. In short

Security and privacy on Graine are shared. Graine runs or supplies the platform; the customer decides how it is used and answers for the people it calls. This document says who does what in each of four deployment models, then lists the controls every customer must operate. Statements are true as of 3 Nov 2026; a control not live for everyone is labelled "Being rolled out" or "Planned". SOC 2 is in progress and no report is held, so section 4 stands in for the customer-side controls a report would list.

2. The four deployment models

	SHARED CLOUD	DEDICATED INSTANCE	YOUR CLOUD ACCOUNT	YOUR OWN PREMISES
Who operates the platform	Graine	Graine	You	You
Compute and data stores	Shared, isolated per workspace	Yours alone	Yours, in your cloud account	Yours, on your hardware
Where call data lives	Graine's platform regions	Region chosen at deployment	Your infrastructure	Your infrastructure
Funding, close-out, metering	Graine's	Graine's	Graine's hosted control plane	Graine's hosted control plane
Air-gapped	Not offered	Not offered	Not offered	Not offered

The last two columns are the public Deployment page's "your compute, our control plane" model, split by where the compute sits. Call audio, transcripts, agent configuration and provider credentials stay inside your network, but three kinds of request still go to Graine over HTTPS: a funding check before each call, the close-out after it, and signed usage and audit events. With the funding gate set to fail closed, losing that connection stops new calls. Neither model is air-gapped. The shared cloud holds compute, agents and call records in India (Mumbai), the API credential store in the United States (N. Virginia) and recordings in the United Kingdom, and does not pin a region per customer.

3. The matrix

"Graine" means Graine does it. "Customer" means the customer does it. "Shared" means both do, split as the note says.

DOMAIN	SHARED CLOUD	DEDICATED INSTANCE	YOUR CLOUD ACCOUNT	YOUR OWN PREMISES	WHAT THIS MEANS
Physical and facilities	Graine	Graine	Customer	Customer	Graine runs no data centres; on the first two models its hosting and storage providers secure them. On the last two they are your cloud provider's or yours.

DOMAIN	SHARED CLOUD	DEDICATED INSTANCE	YOUR CLOUD ACCOUNT	YOUR OWN PREMISES	WHAT THIS MEANS
Infrastructure and network	Graine	Graine	Customer	Customer	Hosts, load balancing, network rules, TLS in front of the API and live-call endpoint. On the last two models you provide the host or cluster and outbound HTTPS, including TCP/443 to Graine; Graine allowlists your egress address.
Platform software and patching	Graine	Graine	Shared	Shared	Graine builds, tests and releases the software. On the last two models you apply releases and patch your hosts; signed release artifacts and a published self-hosted upgrade procedure are not offered. Change scanning and a reviewed deployment pipeline are Being rolled out.
Tenant isolation	Graine	Graine	Shared	Shared	Enforced in the application: a request acts only on the caller's workspace, another's identifier answers "not found", and an automated test checks every route that takes one. A dedicated instance adds compute and databases only you use.
Application configuration (agents, prompts, tools)	Customer	Customer	Customer	Customer	Prompts, voices, tools, knowledge-base documents, campaigns, calling windows, redaction, memory and approvals are yours to set. Graine supplies the controls and defaults.
Identity and access (members, roles, MFA, API keys)	Shared	Shared	Shared	Shared	Graine provides sign-in, roles, custom roles, per-agent access and scoped API keys. You add and remove people, protect secret keys and apply multi-factor sign-in at your identity provider and mailbox. Access reviews are In place (since 4 Nov 2026); authenticator-app sign-in is Being rolled out. Single sign-on is Planned.
Data (content, retention settings, deletion)	Shared	Shared	Customer	Customer	You decide what personal data goes in; Graine stores and protects it. Records are kept until you delete them. Retention settings and finding or erasing one person's data are In place (since 4 Nov 2026). At contract end Graine deletes your data from live systems within 30 days of your written instruction. None of these removes the copy of a call kept in a separate working store.

DOMAIN	SHARED CLOUD	DEDICATED INSTANCE	YOUR CLOUD ACCOUNT	YOUR OWN PREMISES	WHAT THIS MEANS
Encryption keys and secrets	Shared	Shared	Customer	Customer	Providers encrypt stored data; carrier and push credentials sit in a managed secrets store. Customer-managed keys are not offered. You keep your API keys and webhook secrets; hashed API-key storage is Being rolled out.
Logging and audit trail	Shared	Shared	Shared	Shared	Graine keeps a hash-chained audit trail (400 days), the Activity log (CSV export) and the Security log (one year, Being rolled out). You review them and export what you must keep longer. Logging of staff access and of reads of recordings is Being rolled out.
Monitoring and incident response	Shared	Shared	Shared	Shared	Graine monitors the platform it runs and tells an affected customer of a breach within 24 hours of confirming it. It has no staffed 24×7 security operations centre; an incident register is In place (since 4 Nov 2026) and on-call alerts are Being rolled out. You watch your accounts and keys, report a suspected compromise at once and make your own legal notices.
Backup and recovery	Graine	Graine	Customer	Customer	On the shared cloud the primary database is a managed three-node replica set with continuous provider backup and monthly snapshots kept 12 months. It runs in one region with no second site. A dedicated instance is scoped with its own capacity target and is not assumed to be highly available. Restore verification is Being rolled out and the first restore test is Planned by 31 Dec 2026. Recovery targets were set on 3 Nov 2026 (RTO 24 hours, RPO 24 hours; not yet proven by a restore test and not a commitment); a decision on a second site is due by 31 Dec 2026. You back up your own deployment.
Telephony carriers and numbers	Shared	Shared	Customer	Customer	Graine's gateway places calls through carriers. You may use your own carrier account and numbers. Registering and using numbers under telecom rules, including TRAI's, is yours.

DOMAIN	SHARED CLOUD	DEDICATED INSTANCE	YOUR CLOUD ACCOUNT	YOUR OWN PREMISES	WHAT THIS MEANS
Speech and model providers	Shared	Shared	Customer	Customer	Each provider is on the Sub-processor List, with 30 days' notice of changes and a right to object. A provider's use of data is set by its own terms; several use content to improve their models by default, and Graine is opting out wherever a provider allows it. One you connect with your own account is your processor. On the last two models you contract with providers directly.
Legal duties (lawful basis, notices, consent, recording and AI disclosure, do-not-call and telecom rules, parental consent)	Customer	Customer	Customer	Customer	These are yours because you decide why people are called, including a parent's consent for a child (the platform does not check ages). Graine supplies an AI-and-recording notice (off until an Admin sets it; Being rolled out), a do-not-call list (Being rolled out) and a WhatsApp consent record.
Human oversight of agent outputs	Customer	Customer	Customer	Customer	Language models can be wrong. Review outputs before relying on them for decisions about people. Graine supplies approvals, per-agent access, campaign pause, call stop, transfer to a person where the route supports it, a call length cap and optional evaluations.

4. Customer-side controls

Graine's controls assume the customer operates these. Where a customer does not, the protection described in the Security Overview may not hold.

1. **Manage members and roles.** Give least privilege, limit people to the agents they need, remove leavers the same day and review the list regularly: the dashboard records each access review and reminds you every 90 days.
2. **Protect secret API keys.** Keep them on servers, never in a page or app; scope each key; rotate one you suspect and tell Graine at once.
3. **Lock down live end users first.** Before any live end user reaches an agent, turn on "Only my apps", "Require a verified app" and verified users or server tokens. The app and user checks are off until you turn them on.
4. **Verify webhooks.** Check the HMAC-SHA256 signature over the timestamp and exact bytes, use an HTTPS endpoint and keep the secret private.
5. **Set redaction, memory and retention.** Redaction removes phone numbers, Aadhaar, PAN, card numbers and email addresses, not every detail. Memory is off until you enable it and then keeps names and health-related facts by default. Delete data you no longer need.
6. **Use approvals where a mistake is costly.** Another person approves go-live, live-agent edits and campaign launches.

7. **Give notices and obtain consent.** Say it is an AI and may be recorded where the law requires; obtain consent for calls, recordings and transcripts; honour do-not-call and calling-hour rules; obtain a parent's verifiable consent before contacting a child.
8. **Review what agents say.** A person reviews output before it drives a decision about someone; test before go-live; follow the Acceptable Use Policy.
9. **Protect sign-in.** Use multi-factor sign-in at your identity provider and mailbox, since emailed-code sign-in relies on the inbox. Require the authenticator step and single sign-on once live.
10. **Watch the logs.** Review the Activity and Security logs, export what you must keep longer and investigate unexpected changes.
11. **Choose providers and locations knowingly.** Read the Sub-processor List, object within the notice period, and check that recordings in the United Kingdom and other locations suit your law. Choose a dedicated instance or your own compute for one jurisdiction.
12. **Answer people and regulators.** You answer access, correction and erasure requests; Graine helps and passes on any it receives. From 13 May 2027 you tell affected people and the Data Protection Board of a breach without delay, with detail to the Board within 72 hours (Rule 7).
13. **Keep a 24-hour security contact.** A named person and a channel that can receive a breach notice at any hour. Tell founders@graine.ai when it changes.
14. **On your cloud account or premises, run your side.** Patch and back up your hosts, keep outbound TCP/443 to Graine open with generous timeouts, and plan for new calls stopping if it is lost.

Being rolled out, and moving the split as they arrive (as of 4 Nov 2026): authenticator-app sign-in, the AI-and-recording notice and the do-not-call check on every dial. Access reviews, retention controls and data requests by person arrived on 4 Nov 2026. Planned: single sign-on (no date set), and proof of the recovery targets by a first restore test (by 31 Dec 2026). There is no second site today; a decision on one is due by 31 Dec 2026.

5. Contact

Questions about this document or a deployment model: founders@graine.ai.

Related documents

- Security Overview
- Sub-processor List
- Privacy Notice
- Data Processing Agreement: summary
- Responsible AI Statement
- Acceptable Use 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	Correction; the approval of 3 Nov 2026 stands
1.2	2026-11-04	Controls live after the 4 Nov 2026 deploy	Status update; the approval of 3 Nov 2026 stands
1.3	2026-11-04	What erasure, retention and offboarding do not reach stated	Status update; the approval of 3 Nov 2026 stands