Greg - security brief for ICT and CIO review
getgreg.io

What this document is

This brief describes how Greg (getgreg.io) handles meeting recordings for a company that is deciding whether to install it. It states controls that are in the product today, and it states limits that are not yet in place.

Greg has not completed SOC 2 certification or ISO 27001 certification. This document is not a penetration-test report, a HIPAA compliance attestation, or a data-processing agreement. Those require separate legal and audit work.

What Greg records

When a host sends Greg to a Zoom, Google Meet, or Microsoft Teams call, a Recall.ai bot joins as a named participant. The bot's display name is the workspace's bot name (Greg, unless the workspace renamed it). On join, the bot posts a chat message that the meeting is being recorded for the host's workspace and that removing the bot stops the recording. Zoom, Meet, and Teams also show the bot in the participant list.

Bot meetings are transcribed by Recall.ai (recallai_streaming). Audio a person uploads or records in the browser is transcribed by AssemblyAI. The browser recorder tells the person, before capture starts, that audio is uploaded to their Greg workspace.

Greg then stores the audio file (when one is kept), the transcript, the summary, action items, and derived search indexes in the workspace. Calendar auto-join is off unless the workspace turns it on, and an admin can additionally block auto-join for meetings that include someone outside the connected calendar's email domain. Manual join is still a person choosing to send the bot.

Where data lives

Greg is a single-instance application. Production runs on Render in its Singapore region, behind Cloudflare. The database is Supabase-managed Postgres in the Singapore region, and meeting audio is files on the application instance's disk. There is no regional storage selector. Greg does not offer a customer-chosen residency region, a dedicated tenant deployment, or customer-managed keys.

Audio, transcripts, and summaries are not encrypted by the application. Provider OAuth tokens, Slack bot tokens, webhook URLs, Asana personal access tokens, and MCP connector tokens are encrypted with AES-256-GCM. Production startup refuses to boot if that encryption key is missing, weak, or the same value as the session secret, and it refuses to boot without a separate backup key. A workspace's own model key (bring-your-own-key) is encrypted separately. A daily backup archive of the database and meeting files is encrypted with AES-256-GCM and kept for 30 days. It is written to the same host volume. Copying it off the

host is supported but is not described here as in place. The live host volume is not encrypted by this application. A restore drill script is in the repository; it has not been run against production from this change.

Traffic between the browser and Greg uses HTTPS in production. Session cookies are httpOnly, SameSite=Lax, and Secure in production. A session lasts 30 days. Signing a user out of a deleted account revokes that user's server-side sessions.

Who can access a meeting

Meetings belong to one workspace. A member sees a meeting they own, a meeting with no owner (legacy), a meeting explicitly shared with them, or a non-private meeting shared with the whole workspace or inherited from a board they can see. Private meetings are visible to the owner and to people named on a per-person share. A whole-workspace share does not open a private meeting.

Workspace API keys are read-only and org-wide. By default they cannot read private meetings or their transcripts or tasks that came from a private meeting. An admin can mint a key with the meetings:private scope when a specific integration needs that content. Keys are stored as a SHA-256 hash. The secret is shown once.

A share can name a current member of the same workspace, or the whole workspace. It cannot name a user from another workspace. When a member is removed, their per-user shares are deleted. Shared-password (single operator) login is disabled in production. Sessions issued on that path are rejected.

Greg's assistant (in-app chat, Slack, SMS, WhatsApp, phone and voice) answers from a meeting only when the person asking can open that meeting. Prep screens, mobile focus cards and public clip data use the same check. A person who cannot open a meeting gets the same response as for a meeting that does not exist.

Briefs, Debriefs and meeting prep only draw on meetings the reader can open; anything sent to a shared channel uses only meetings shared with the whole workspace.

A signed-in API request with a logged-out session or a deleted account gets 401, not an empty answer.

Subprocessors the product calls

Recall.ai - joins Zoom, Google Meet, and Teams, captures the recording, and transcribes bot meetings. When a meeting is deleted, Greg asks Recall to delete that bot's stored media. If the bot id is missing or Recall does not acknowledge the delete, the deletion job records unavailable or failed. It does not claim the vendor copy is gone.

AssemblyAI - speech-to-text for uploaded and browser-recorded audio. Not used for bot meetings. Greg stores the AssemblyAI transcript id and calls their delete endpoint on

meeting delete. Meetings transcribed before that id was stored are recorded as unavailable.

OpenRouter - primary path for summaries, extraction, and the assistant's tool-using conversations. The default model is a DeepSeek model hosted through OpenRouter. The product does not send GPT model names through OpenRouter.

Anthropic - automatic fallback when OpenRouter is unset or unavailable, and the pinned path for a claude-* re-run. A workspace admin can turn this fallback off. If no permitted provider is available, the call fails.

OpenAI - used by default through the platform task router for background classification, fallback wording, and higher-judgment planning. A workspace admin can turn off the platform OpenAI router in Settings, Security. A workspace's own OpenAI key is separate, and that key is still used when the platform router is off. The environment variable AI_ROUTER_ENABLED=false turns the platform router off for the whole process.

Google Gemini - embeddings for meeting search, and realtime voice for the in-meeting assistant and phone bridge. Not used for summaries. A workspace admin can turn Gemini off. Those features then fail closed instead of sending content.

Google - Calendar connect requests calendar, email, profile (for the signed-in photo), and openid. contacts.readonly (photos of saved contacts) is added only when GOOGLE_CONTACTS_SCOPE=1. Gmail and Drive scopes are requested only when an admin has allowed that integration and a person starts that grant (?gmail=1 or ?drive=1). A grant without profile still works and shows initials. Sign-in OAuth requests openid, email, and profile, and does not keep a Google access token. Gravatar is off unless GRAVATAR_AVATARS=1, because that sends an email hash to a third party.

Microsoft - Outlook calendar and mail when a member connects Microsoft 365. Sign-in OIDC is a different grant and is not reused for mail.

Twilio - SMS, WhatsApp, and phone calls when the workspace turns those channels on. A stored phone number is not consent to call.

Resend - transactional email, including meeting summaries.

Stripe - subscription billing. Greg does not store full card numbers.

Slack, HubSpot, LeadConnector, Asana, and Zapier - only if an admin connects them. Notes are not pushed to a CRM or Slack channel the workspace did not connect.

Render - application hosting and storage (Singapore).

Supabase - managed Postgres database (Singapore).

Cloudflare - DNS, TLS and edge network in front of getgreg.io.

PostHog - product analytics and error capture, sent through a first-party /ingest proxy.

Apple - push notifications and Sign in with Apple for the iOS app.

Greg does not use customer meeting content to train Greg's own models. Whether a subprocessor trains on data sent to its API depends on that provider's terms and the account configuration. Those terms are not certified on this page.

Retention, deletion, and export

Meetings stay until someone deletes them, unless a workspace admin sets a retention period in Settings, Security. Each delete and each purge writes a deletion job id. The job removes the meeting row, shares, search chunks, the local audio file, and clip images, appends the meeting id to a deletion ledger outside the database, and asks Recall and AssemblyAI to delete their copies when Greg has an id to send. A failed location stays on the job and is retried. A missing vendor id is unavailable, not a silent success. There is no separate free-plan job that hides old meetings while leaving them in the database.

Public clip links expire. The default lifetime is 30 days, and an admin can change it or set it to zero so clip URLs stop working. Private meetings are never served on a public clip URL. An admin can also turn off external sharing, which disables public clip URLs and drops summary-email recipients who are not members of the workspace. Deleting a meeting removes its clips.

Deleting an account signs the user out and stops processing right away. The account is permanently deleted 14 days later and can be restored from the website until then. Deleting a user who is the only member deletes that workspace's meetings and connected-app tokens from Greg's database, then the user. Deleting a user who shares a workspace removes that person and their private meetings. It does not delete the workspace's other meetings. A restored database snapshot can contain meetings deleted after that snapshot was taken. scripts/restore-drill.ts reapplies the deletion ledger so those meetings are removed again. The backup script keeps at most BACKUP_LOCAL_KEEP local archives (default 3) and deletes local archives older than the backup window (30 days unless BACKUP_RETENTION_DAYS is set). After a successful off-site upload it also deletes off-site archives older than that window, except the newest 3. The off-site deletion ledger object is kept.

An admin can export the security audit log as CSV from Settings, Security. The product's meeting pages are the export of a transcript the viewer is allowed to open. There is no legal-hold or eDiscovery package.

Admin controls and audit

Workspace admins manage members, API keys, integrations, auto-join, bot name, retention, public clip lifetime, model-provider approval (OpenRouter, Anthropic, Gemini, and the platform OpenAI router), Gmail and Drive consent, downloads, summary email, CRM and Slack

delivery, external sharing, and the external-meeting auto-join block. Org-wide configuration changes are rejected for non-admins. A host can stop a live bot from the meeting page. That calls Recall leave_call and writes capture.stopped.

The audit log records capture start, capture skipped by the external-meeting policy, capture stopped, meeting delete, share changes, API key create and revoke, transcript reads, exports, private and ordinary reads through the workspace API, audio playback, retention purges, denied deliveries, and security-policy changes. Transcript and notes reads through the assistant are written to the audit log. Transcript reads and exports are recorded once per actor per meeting per hour so the meeting page poll does not flood the table. Each row has an actor (when a person did it), an action, an object id, a timestamp, and a source. The row does not contain the transcript or the token.

The log is an ordinary table in the same Postgres database. It is not an immutable external ledger. It is kept until the workspace is deleted.

What is not in place

No SOC 2, ISO 27001, HIPAA, or independent penetration test is claimed.

No SSO with a customer’s identity provider, no SCIM provisioning, no customer-managed encryption keys, and no enforceable regional processing.

No application-level encryption of audio, transcripts, or summaries. Encrypted backup archives are produced by the backup script. A production restore drill has not been recorded as deployment-verified.

No contractual data-processing agreement is included with the product download. Ask hello@getgreg.io for contract terms.

No multi-factor authentication for email and password sign-in.

No independent penetration test or public bug bounty.

Reporting a security issue

Email hello@getgreg.io with ’Security’ in the subject. Include steps to reproduce and the affected URL or app version. Please give us reasonable time to fix an issue before disclosing it, and do not access, change or delete other people’s data while testing. We will acknowledge the report and keep you updated. There is no paid bug bounty.

Planned

None of the following is available today. No date is attached to any of them.

SSO (SAML/OIDC) with a customer’s identity provider. Planned. Not available today.

SOC 2. Greg is a pre-seed company, and certification comes later. Planned. Not available today.

Closing the remaining per-viewer gaps. Planned. Not available today.