



Security and Data Privacy

Public overview, prepared for prospective customers and security reviews

Version 1.2 (public). Last reviewed June 2026.

June's whole design is a small footprint: nothing recorded in front of your customer, nothing kept after the CRM write, and your system of record stays the only system of record. This document is the public overview. Detailed, vendor-named architecture documentation is available on request under NDA at it@calljune.ai.

How CallJune works

A sales rep calls June from their phone after a meeting. No app, no login, and no recording of the original meeting. The rep talks through what happened, June asks the questions and structures the answers, and the result is written directly to the rep's CRM (HubSpot, Salesforce, or another supported CRM) through its standard API. The call audio and transcript are processed in real time and deleted after the CRM write completes.

Authentication

CallJune uses phone-based two-factor authentication:

- Factor 1 (something you have): the rep's registered phone number. Calls from unrecognized numbers are not processed.
- Factor 2 (something you know): a unique per-rep PIN spoken at the start of each call, validated before any CRM data is loaded or any processing begins.

Each rep is scoped to their own CRM identity and can only access and update records they own.

How data moves, and what is kept

- Rep calls June from a phone.
- Voice is processed by a SOC 2 Type II voice platform configured to store no recordings and no transcripts. Limited call metadata is retained for a short audit window, then auto-deleted.
- The transcript is passed to the CallJune processor (SOC 2 Type II hosting), where an AI model extracts structured CRM actions.
- Structured data is written to the CRM through its standard API (OAuth 2.0, your own per-organization credentials). Only the rep's owned records are read or modified.
- Post-write cleanup: the transcript and audio are deleted from CallJune systems and from the voice platform. Only the CRM-ready structured data persists, in your CRM.

End state: after processing, the rep's call data exists only in your CRM, where you control retention, access, and compliance. CallJune retains no recordings, no transcripts, and no raw call audio.

Infrastructure security

Every system in CallJune's data path holds independent SOC 2 Type II certification. Specific providers are described by category here; named detail is available under NDA.

Layer	Role	Certification
Orchestration platform	Workflow orchestration	SOC 2 Type II
Voice platform	Voice agent processing	SOC 2 Type II, HIPAA BAA available
Application hosting	Application hosting	SOC 2 Type II, ISO 27001
Database and auth	Data store and authentication	SOC 2 Type II, HIPAA BAA available

AI model providers

CallJune supports multiple AI model providers for transcript analysis. None use API data for model training.

Provider	Trains on API data?	Retention
Anthropic (Claude)	No (default)	7 days, then deleted
OpenAI	No	30 days, then deleted
Google (Gemini)	No (paid tiers)	Per agreement

The model provider can be selected by customer preference. Zero Data Retention agreements are available from all three providers for enterprise customers.

Per-user data isolation

- Each rep is authenticated by phone number and PIN before any data is accessed.
- CRM queries are scoped to the authenticated rep's owner ID. A rep cannot read or modify another rep's records.
- Structured outputs are tagged with the rep's identity and the customer organization. Cross-organization data access is not possible at the application layer.
- Database queries are filtered by organization ID and rep ID at every access point.

What CallJune does not do

- Does not record the original sales meeting. The rep calls June after the meeting; the meeting itself is never recorded or monitored.
- Does not store call recordings. Audio is discarded after processing.
- Does not store call transcripts. Transcripts are used for real-time extraction, then deleted.
- Does not use customer data for AI training. API-tier agreements with all model providers prohibit it.
- Does not require an app, browser, or internet login. Authentication is phone-based only.

Compliance roadmap

Milestone	Status
All infrastructure layers SOC 2 Type II certified	Complete

AI model providers: no-training API policies confirmed	Complete
Configurable data retention per customer	Complete
Programmatic post-processing data deletion	Complete
CallJune application-layer SOC 2 Type I	In progress
CallJune application-layer SOC 2 Type II	Planned (following Type I)

Contact

For security questions, questionnaires, or detailed vendor-named documentation (shared under NDA):
it@calljune.ai

Shawn Johnson, Founder, CallJune.ai. Dragan Jovanovic, Engineering Lead.

Public security overview. Detailed, vendor-named architecture is available on request under NDA. CallJune.AI, a Ready Voice AI LLC company, Irvine, CA.