PipeGuide — Security & Architecture Overview

Technical briefing for IT decision-makers · app.pipeguide.tech · June 2026

ARCHITECTURE AT A GLANCE

LAYER	TECHNOLOGY	ROLE
Frontend	React (SPA)	Rep live-call screen, manager analytics, admin console
Backend	FastAPI (async Python)	Stateless REST API, horizontally scalable
Database	MongoDB	Multi-tenant document store — orgs, users, transcripts, billing
Hosting	Managed Kubernetes	TLS-terminated ingress, isolated pods, custom domain

CONNECTED SERVICES & WHAT EACH ONE SEES

SERVICE	PURPOSE	DATA EXPOSURE
Recall.ai	Meeting bot (Zoom / Teams / Meet / Webex), live transcription, optional read-only calendar sync	Meeting URL, call audio, transcript; calendar events if connected. No AI training on customer data; calendar events auto-purged after 60 days
Deepgram	Live speech-to-text for in-person / phone mode	Microphone audio stream only
OpenAI (GPT-5.2)	Live qualification scoring, suggested questions, post-call summaries	Transcript text only — API tier, **not used for model training**
Paystack	Subscription billing & usage packs (ZAR)	Card data handled entirely by Paystack — never touches PipeGuide (PCI stays with Paystack)
Google / Microsoft OAuth	SSO sign-in; optional read-only calendar	Email, name; upcoming event metadata only — never writes to calendars
Resend	Transactional email (verification, coaching digests, reminders)	Recipient email + report content
Object storage	Logos & catalogue uploads	Files only, organisation-scoped

AI data governance: calendar / Workspace data is architecturally isolated from AI — it is never included in any AI model input (code-enforced, and publicly disclosed in our privacy policy per Google's Limited Use requirements). No call recordings are stored — only transcripts and summaries, owned by your organisation.

MULTI-TENANCY & DATA ISOLATION

- Every record carries an organisation ID; **every API query is scoped server-side** to the authenticated user's organisation — cross-tenant access is impossible by construction, independently audited across all endpoints
- Role-based access: Admin (configuration, view-only on calls) · Manager (department-scoped analytics) · Sales rep (own calls only)
- Compound database indexes on the tenant key keep isolation performant at scale

SECURITY CONTROLS

- **Authentication:** JWT access + refresh tokens in httpOnly secure cookies (XSS-resistant); optional Google SSO; token versioning for instant global session revocation
- **Passwords:** bcrypt hashing; 6-digit email verification at signup; disposable-email domains blocked
- **Brute force:** 5 failed attempts → 15-minute lockout per IP + email
- **Rate limiting:** per-endpoint limits across auth, uploads and AI routes
- **Secrets at rest:** third-party credentials encrypted (Fernet / AES-128) before storage
- **Webhooks:** payment & bot callbacks verified with HMAC signatures — forged events rejected
- **Headers:** strict Content-Security-Policy; TLS / HSTS at ingress
- **Audit logging:** administrative and platform actions recorded with actor + timestamp

DATA LIFECYCLE & COMPLIANCE (POPIA-AWARE)

- Call recordings are **not stored** — transcripts and AI summaries only, owned by your organisation and exportable as PDF
- Offboarding: suspend → terminate (data retained for a configurable retention window) → hard purge with full cascade across all collections; irreversible deletion requires typed confirmation
- Calendar access is revocable in-app at any time; synced events are deleted on disconnect
- All sub-processors publicly disclosed in the privacy policy, including the Google Limited Use compliance statement
- Google OAuth verification submitted; Microsoft publisher verification in progress

RELIABILITY & SCALE POSTURE

- Stateless API behind managed ingress — horizontal scaling without session affinity
- Token-metered usage provides built-in per-tenant cost and abuse control
- Transparent roadmap item: live-event pub/sub is in-memory today; Redis is the planned swap for multi-node scale — a configuration-level change, not a re-architecture

COMMON CIO / CTO QUESTIONS

QUESTION	ANSWER
Do you train AI on our data?	No. All AI providers run on no-training API tiers, and calendar data never reaches AI at all.
Can another customer see our data?	No — organisation-scoped queries are enforced server-side on every endpoint.
What happens if we leave?	Your organisation can be terminated and hard-purged on request; PDF summaries are exportable beforehand.
Where does call audio go?	Streamed for live transcription, transcribed, then discarded — no recordings at rest.
Who can start recording a call?	Only the sales rep, explicitly, per call — and the bot is a visible participant in the meeting.
How are payments secured?	Paystack handles all card data; PipeGuide never stores payment details and verifies every webhook signature.

Questions? Our team is happy to walk your IT stakeholders through a live architecture review or complete your security questionnaire. Contact us via app.pipeguide.tech.