Klarissa.AI

PhoneAI Technology & Security Overview

(Updated April 2025)

1 | Purpose of This Document

This overview explains how Klarissa.AI's PhoneAI platform handles telephone calls, data transmission, storage, security, and access permissions. It is intended to give current and prospective customers confidence that our technology is robust, private, and resilient.

---

2 | What PhoneAI Does

- **Always-on voice assistant** – Answers inbound calls, understands the caller's request, executes approved actions (for example, sending a text message), or routes to staff when needed.

- **Accurate conversation handling** – Uses Speech-to-Text (STT), a Large-Language-Model engine, and Text-to-Speech (TTS) to hold natural multi-turn dialogues based on your organization's knowledge base.

- **Comprehensive logging** – Captures call metadata including but not limited to caller phone number, timestamp of call, duration of call, call summary and call transcript for quality review.

- **Single-tenant visibility** – Each customer sees only their own calls and insights in a secure dashboard.

---

3 | High-Level Architecture

1. **Call arrival** – A caller dials your published number. Telephone traffic forwards to Klarissa.AI via Signaling System 7 (SS7) for landline and mobile phone networks or via Session Initiation Protocol (SIP) trunks for Voice over Internet Protocol (VoIP) providers; both paths are encrypted in transit.

2. **Secure media gateway** – Audio is protected with Transport Layer Security 1.2 or higher (TLS 1.2+) and Secure Real-Time Transport Protocol (SRTP).

3. **Speech processing** – Audio is converted to text by the Speech-to-Text engine; no raw audio is stored by the speech vendor.

4. **Conversation logic** – Text passes to a containerized Large-Language-Model that follows customer-specific instructions and retrieves answers from your knowledge base or approved application programming interfaces (APIs).

5. **Response generation** – The model's reply is converted back to speech by the Text-to-Speech engine and played to the caller.

6. **Data capture** – Metadata and transcripts are saved in your dedicated database instance; transcripts reside in a sandbox for up to 30 days (security review) before deletion or transfer to your own storage.

---

4 | Data Protection Measures

Aspect	Controls in Place
Encryption in transit	All web, API, and voice traffic uses Transport Layer Security 1.2+ (TLS 1.2+) or better.
Encryption at rest	Databases, object storage, and backups are encrypted with Advanced Encryption Standard 256-bit (AES-256).
Tenant isolation	Every customer has a separate Virtual Private Cloud (VPC), subnet, and PostgreSQL instance; network Access Control Lists block cross-tenant traffic.
Data retention	Caller data—including but not limited to caller phone number, timestamp, duration, call summary and call transcript—is retained in line with the laws, policies, or best practices of the customer. Data can be securely archived: archived records remain encrypted and searchable for compliance while limiting the amount of data visible in day-to-day dashboards.
Ownership	Customers own 100 percent of their call data; Klarissa.AI never uses it to train external models.

---

5 | Identity, Access & Permissions

- **Role-Based Access Control (RBAC)** – Admin, Analyst, and Read-only roles restrict what users can view or change.
- **Multi-Factor Authentication (MFA)** – Enabled upon request for the web dashboard.
- **Single Sign-On (SSO)** – Optional Security Assertion Markup Language 2.0 (SAML 2.0) integration to your identity provider.
- **API security** – OAuth 2.0 bearer tokens scoped to least privilege; rotating secrets recommended.
- **Audit trail** – Every login, export, and configuration change is written to an immutable log. Reports can be provided on request or on a schedule defined in your Master Services Agreement (MSA).

---

6 | Platform Monitoring & Incident Response

Capability	Details
Real-time monitoring	24 × 7 automated alarms on system health, performance, and anomalous activity.
Vulnerability management	Weekly scans; critical issues patched within 72 hours.
Penetration testing	Penetration testing performed annually; summary report available under non-disclosure agreement.
Incident response	National Institute of Standards and Technology Special Publication 800-61 playbook; customer notified within 72 hours of any confirmed breach.
Disaster recovery	Active-active deployment across multiple cloud availability zones, daily encrypted backups, quarterly fail-over drills.
Service Level Agreement (SLA)	99.5 percent monthly uptime with service-credit remedies for extended outages.

---

7 | Artificial-Intelligence Safeguards

- **Input sanitization** – Removes control sequences and suspicious patterns to block “prompt injection.”
- **Sandboxed execution** – Large-Language-Model runs in a locked-down container with no direct database credentials.
- **Output moderation** – Filters ensure replies do not leak personal data or disallowed content.
- **Red-team testing** – Quarterly adversarial exercises probe for bias, toxicity, or jailbreak vectors.
- **No training on live data** – Call transcripts are excluded from future model training unless a customer explicitly opts in.

---

8 | Compliance Foundations

- **General Data Protection Regulation (GDPR)** and **California Consumer Privacy Act (CCPA)** – Klarissa.AI acts as a Data Processor and supports data-subject requests.
- **National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)** – Internal controls mapped and reviewed twice a year.
- **Financial Information Processing** – Klarissa.AI does not accept or store credit-card details or other confidential financial or personal data from callers.
- **Telephone Consumer Protection Act (TCPA)** – Outbound features enforce consent, Do-Not-Call list scrubbing, and opt-out handling.

---

9 | Customer Responsibilities

1. Safeguard administrator and user credentials; enable Multi-Factor Authentication (MFA) if required.

2. Obtain and document any required caller consent for call recording, artificial voice, or outbound dialling.

3. Review your own retention and deletion schedules in the Klarissa.AI dashboard.

4. Vet and approve any third-party integrations you connect to PhoneAI.

5. Notify Klarissa.AI promptly of any suspected security incident or credential compromise.

---

10 | Support & Contact

- **Email support** – support@klarissa.ai
- **Support portal** – Accessible through your Klarissa.AI dashboard.
- **Security audits** – Request the latest penetration-test summary or compliance questionnaire via your account manager.

Klarissa.AI is committed to keeping your callers' information private, your data secure, and your service available.

For any questions about this overview, please contact **support@klarissa.ai**.