Security Overview

Sakshi · AI agent governance | Version 1.0 | July 2026

Sakshi is the governance layer for AI agents in Indian enterprises: it registers every agent, records every decision on a tamper-evident chain, bounds what agents may do on their own, and turns that into regulator-mapped evidence. This overview describes how it is secured. The short version: Sakshi is single-tenant and runs inside your environment, so the deployment model is the security model.

Tenancy	**Single-tenant**	Runs in	**Your VPC / on-prem**
Raw PII stored	**None**	Vendor data access	**None**
Evidence integrity	**Hash-chained, signed**	Data residency	**India by default**
Identity	**SSO / OIDC / SAML**	Components	**Open, Apache-2.0**

01 Isolation and data model

The strongest control we offer is architectural. Sakshi installs in your environment and stays there, so the question of what a vendor could do with your data mostly does not arise.

- **Single-tenant.** Each customer runs their own instance in their own VPC or on-prem. No shared control plane and no multi-tenant database, so there is nothing shared to isolate between customers.
- **No call-home.** The platform does not phone Rotavision. It runs entirely within your network boundary, works air-gapped, and gives you nothing to allow-list outbound.
- **Residency by default.** Because it runs where you put it, residency is yours to set. India by default; wherever your policy requires otherwise.

02 Data handling

Sakshi is an evidence system, not a system of record for your sensitive data. It governs the act and holds the proof; it never becomes the place your raw identifiers live.

- **PII tokenized at ingest.** Personal identifiers are replaced with reference tokens before a record is written. Raw Aadhaar, PAN, card, and account numbers never enter the decision chain, so the evidence is defensible and the sensitive value is not sitting inside it.
- **Keys stay with the deployment.** The signing seed and tokenization configuration live in your instance, under your control. We cannot detokenize your records or forge a signature, because we do not hold the material to do so.
- **Encryption.** Traffic is TLS-encrypted. At rest, evidence sits on your infrastructure and inherits your storage encryption and key management, because it is your infrastructure.
- **Vault-verified disposition.** Where a raw identifier must be stored, Sakshi verifies it landed in a compliant vault (for example a UIDAI-style Aadhaar Data Vault) by its reference key, without ever seeing the value.

03 Integrity and independent verification

Every decision is hashed into a chain where each record seals the one before it. Recomputing the chain re-derives every hash, so tampering with a single field is not just detectable, the chain says exactly where it happened. Evidence packs are Ed25519-signed over their exact bytes. Your security, compliance, and audit teams do not have to take Rotavision's word for the integrity of a record, and neither does your regulator.

04 Access, identity, and operations

- **SSO and RBAC.** SAML and OIDC single sign-on against your IdP (Keycloak, Okta, Entra, Google Workspace). Role-based access with a read-only auditor role, mapped from your directory.
- **Separation of duties.** Who can approve a high-autonomy action, mint an ingest key, or administer the platform are distinct roles. Entitlement changes are themselves attested on the chain.
- **Audit logging and export.** Privileged actions, kill-switch activations, and drills are recorded as evidence. Signed packs and full chain exports are available on demand.
- **Resilience.** Nightly evidence backups, a drilled kill switch with signed attestations, and one-command install and upgrade via Helm or docker-compose, on your schedule.

05 Compliance, provenance, and certifications

Sakshi is built to **produce** regulator-grade evidence and is DPDP-aligned by design (tokenization, minimization and localization screens, and an independent-auditor bundle). Its clause maps cover RBI Model Risk Management, DPDP, SEBI Regulation 16C, and anticipated IRDAI guidance.

On formal certifications, we are deliberately plain: **SOC 2 Type II and ISO 27001 are on our roadmap, not yet in hand.** We will state so here when they land, and we will not imply them before. Our governance models and SDKs are open and Apache-2.0 licensed, so the components you run are inspectable rather than taken on trust.

06 Responsible disclosure

We would rather you check than take our word for it. If you believe you have found a security issue, email security@rotavision.com with details and steps to reproduce. We acknowledge reports, work them in good faith, and credit researchers who want it. Please test only against your own sandbox or deployment.

This overview describes Sakshi's architecture and controls and is suitable for an initial vendor-risk review. A fuller pack, including a completed security questionnaire and a data processing addendum, is available on request under NDA; audit reports will be added as certifications mature. Request it at security@rotavision.com or via rotavision.com/contact.

Rotavision Consulting Private Limited · AI Trust Infrastructure for India
WeWork, HD-37, Block D3, Manyata Tech Park, Bengaluru 560045, Karnataka, India
rotavision.com · hello@rotavision.com · security@rotavision.com