Rokan: security and data

For the engineer deciding whether a two-week trial is safe. Every line is something the product does today.

> **Where we are, plainly.** Rokan is an early company. We are not SOC 2 certified and have no customers yet. So the trial is built to need as little of your data as possible, or none of it leaving your side.

Two ways to run a trial

	Shared runs (default)	Strict mode
What we see	Only the runs you choose to send	Nothing. It runs on your machine or in your cloud
Model	Claude, through Anthropic's API (Anthropic does not train on API data)	A model on that machine only (for example Ollama or vLLM on localhost)
Network	Model calls only	None from Rokan: its process refuses outside connections and DNS lookups. For a hard guarantee, run it with networking turned off
What leaves	The runs you picked, with personal details removed by us before anything is stored	Nothing, unless you choose to send us the report

What protects your data

- **Strict mode refuses outside connections.** A guard inside Rokan's process refuses any connection or DNS lookup to anything other than the local machine, and the tool refuses webhooks, remote deploy hooks and executable hooks. This is covered by automated tests. The guard covers Rokan's own process, not programs it starts (such as git), so for a hard guarantee run it in a container or VM with networking turned off.
- **Model allowlist.** A deployment can be limited to an allowlist of model hosts; a call to any other host is refused before a byte is sent, and the refusal is logged. Strict mode limits it to the local machine.
- **No training on your data by default.** What Rokan learns is kept as outcomes, not conversation text, unless you turn that on, and nothing trains a model on your data without your written opt-in.
- **Nothing ships on its own.** A fix arrives as a suggested change or a local git branch. It goes live only when someone on your team approves it; we never push to your repo.
- **Deletion.** We delete what you send within 30 days of receiving it, or any time you ask.
- **Shared runs are scrubbed on arrival.** Names, phone numbers, emails, addresses, IDs and card numbers are replaced before anything is stored, and the original export is never copied. You can still remove anything else you'd rather we didn't see.

What we don't have yet

A SOC 2 report, a pen test, a BAA. If your review needs any of these before a trial, strict mode is the way to start, since none of your data reaches us.

Arav Kekane, Rokan · rokan.computer · aravkekane@gmail.com