AI & Your Data

How Theama protects each customer's data when using AI · CloudKnots Ltd · Last updated 7 November 2026

Our guiding principle: we never rely on the AI to police its own boundaries. Isolation is enforced by the architecture around it — signed identities, per-tenant data scoping, and strict data minimisation — so your data stays yours.

1. The AI advisor is private — not a public feature

The live AI advisor is available only to logged-in owners and their invited team. Every request is authenticated against your signed session and metered against your plan's AI credits, and it only ever analyses your own account's data. The only place AI appears on a public (logged-out) page is our interactive demo, which shows pre-written sample answers on fictional data — it makes no real AI model call and uses no real business data, so nothing of yours is ever exposed on a public surface.

2. Your identity is proven on every request

Access is controlled by a cryptographically signed token issued at login and verified on our servers for every request. Your data boundary derives from that token — it cannot be spoofed or overridden by anything sent from a browser or app. Sessions run over TLS and can be revoked across all devices instantly.

3. Your data is only ever queried within your own account

Every dashboard metric, integration credential, and AI conversation is stored and retrieved scoped strictly to your account and team. One customer's request can never reach another customer's data, and we never pool different customers' data into a shared store or index.

4. The AI only ever sees a minimal, aggregated snapshot

The advisor receives only high-level summary figures (e.g. "YTD revenue", "security score") assembled on our servers from your account only — never raw customer lists, invoices, contact details, or account numbers, and never another customer's data. The AI has no database access and cannot run queries or tools, so it is architecturally incapable of reaching another tenant's data.

5. Deterministic guardrails around every AI request

Every question is screened — attempts to extract system instructions, raw records, or another customer's data are blocked before reaching the model. Every response is redacted — emails, card/account numbers, and similar identifiers are stripped automatically. Every AI request is logged — owners can review a full, timestamped audit log of their team's AI activity in-app.

6. Your data is not used to train models

Summary metrics are sent through our managed key to the AI model provider's API as a private, per-request call — not a shared or public chatbot — solely to generate your insight, under contractual confidentiality and no-training / no-retention terms. Our staff do not read your AI conversations except with your consent, for security, or to comply with law.

7. What we don't do

We do not sell your personal or business data. We do not pool tenants' data into a shared index or model. We do not let the AI read your raw records or reach another tenant's data.

Questions? Contact hello@cloudknots.com. This one-page summary may be shared with your compliance or security team. © CloudKnots Ltd.