AgentsBooks — Security & Trust Overview

Generated 2026-11-23 from the live Trust Center.

Canonical source: https://agentsbooks.com/security

This file is a point-in-time snapshot of a page that changes.

Before relying on it in a review, check the canonical URL above.

Infrastructure

- AgentsBooks runs on Google Cloud Run (Google Cloud Platform).
- Google Cloud's data centres hold SOC 2 Type II, ISO 27001 and ISO 27017 certifications. Those are Google's certifications, covering the infrastructure we build on — they are not an AgentsBooks attestation and we do not present them as one. AgentsBooks' own SOC 2 status is in the section below.
- Encryption in transit (TLS 1.2+) and at rest. Strict per-tenant isolation.

Third-party assurance

- SOC 2 Type II — an independent audit is underway. All Common Criteria controls (CC1–CC9) are implemented and operating; the attestation letter has not yet been issued. We do not name the firm here until the engagement is one we can attribute.
- Penetration test — not yet commissioned with a firm we can name. We would rather record that than imply a test we cannot cite.

Data protection

- GDPR and CCPA posture documented at https://agentsbooks.com/privacy
- DPA available on request: https://agentsbooks.com/contact?subject=dpa
- Audit log retention: 365 days, exportable.
- Vulnerability disclosure: https://agentsbooks.com/security/disclosure
- Live status: https://agentsbooks.com/status

Sub-processors

Effective date: 2026-10-06. We give 30 days' notice of changes.

Always-current register: https://agentsbooks.com/subprocessors

Machine-readable: https://agentsbooks.com/subprocessors.json

CSV: https://agentsbooks.com/security/subprocessors.csv

Sub-processor | Purpose | Location

Google Cloud Platform | Infrastructure & compute | US (us-central1); agent runs also us-east1, europe-west1, me-west1

Auth0 (Okta) | User authentication | US

Stripe | Payment processing | US

OpenRouter | AI model gateway — the default route for chat and agent requests, forwarding each one to the model you selected | US

Anthropic | AI model provider (Claude) | US

OpenAI | AI model provider (GPT) | US

Google (Gemini) | AI model provider | US

DeepSeek | AI model provider — engaged only when you connect a DeepSeek key or select a DeepSeek model | China (PRC)

Other model vendors via OpenRouter | AI model providers reachable through the gateway (for example Meta, Mistral, xAI, Qwen and other hosted open-weight models) — engaged only when you select one of their models | Varies by vendor

Cloudflare | DNS & CDN | Global

Contact

Security questions: https://agentsbooks.com/contact?subject=security