

Platform Security

Your data lives on secure cloud infrastructure, backed by policy best practices, verified by audit, safety by design.

SOC 2 TYPE II

Independently audited security

CompScience maintains a SOC 2 Type II report across key trust categories: Security, Confidentiality and Availability. Third-party audit confirms that our controls are not just designed correctly but keep working correctly over time.

ENCRYPTION AND INFRASTRUCTURE

- Data encrypted in transit (TLS 1.2 or higher), and at rest (AES-256).
- Auditable AWS infrastructure provisioned with Terraform.
- Continuous monitoring and vulnerability scanning.

POLICIES AND GOVERNANCE

- Endpoint protection on employee devices.
- Internal access limits. Only authorized staff can reach customer data.
- Annual SOC 2 audits.
- Regular third-party penetration testing.
- Over 30 documented information security policies, annual employee training.

PRIVACY AND TERMS OF SERVICE

Privacy Policy compscience.com/privacy-policy	Terms of Service compscience.com/terms-of-service	CCPA Notice compscience.com/california-privacy-rights-policy	GPC Policy compscience.com/global-privacy-control-policy
---	---	--	---

Cloud AI and Data Protection

Certain features require advanced reasoning or visual processing. For these, CompScience may use frontier models from three leading AI providers: Anthropic, OpenAI, and Google. All three are governed by contracts and attestations that explicitly prevent indefinite retention and training on your data.

FAQ

Do the AI providers used by CompScience train their models on our data?

No. CompScience only uses business tiers across all three providers. Each have explicit contractual commitments not to train their models on data sent through these APIs.

Could our data show up in another customer's AI response?

No. Because the providers don't train on CompScience's data, that data cannot influence what other customers see. Inputs are processed for the request, returned, and not retained for training.

How is the use of AI providers different from any other technology provider?

It isn't. The contracts, audits, and encryption standards used by AI providers are the same ones already governing cloud infrastructure industry standards — SOC 2, ISO 27001, GDPR DPAs.

AI PROVIDERS ENSURE YOUR DATA IS IN SAFE HANDS

- **Paid business tiers only.** CompScience never uses the free / consumer tier of any AI provider, where data may be used for training.
- **Encryption end to end.** Data is encrypted in transit (TLS 1.2+) and at rest (AES-256) by every provider.
- **SOC 2 reports on file.** Independently audited security reports from each provider.
- **Data is not retained by 3rd parties.** Providers keep inputs and outputs only for a limited period, solely for abuse monitoring and legal compliance, then delete them. None of it trains a model or goes to a third party, except where law requires longer retention. Each provider publishes its current retention window: [Anthropic](#), [OpenAI](#), and [Google](#).

WHAT EACH PROVIDER COMMITS TO, IN WRITING

PROVIDER	TRAINING ON BUSINESS/API DATA	SECURITY STANDARDS	SOURCES
Anthropic Claude API	No. Commercial Terms state Anthropic may not train on Customer Content from the Services.	SOC 2 Type 2, ISO 27001, ISO 42001	Commercial Terms Is my data used for training? trust.anthropic.com
OpenAI OpenAI API	No. API data not used to train models since March 1, 2023 unless you opt in.	SOC 2 Type 2, ISO 27001, ISO 42001	API data usage Enterprise Privacy trust.openai.com
Google Gemini API, paid	No. On paid services, prompts and responses are not used to improve Google products.	SOC 2 Type 2, ISO 27001, ISO 42001	Gemini API Terms Google Cloud compliance