

Data Security & Compliance

Designed for regulated industries from day one

Most frontier AI models (Claude, GPT, Gemini) are designed for broad consumer use. Without specialized enterprise agreements, anything entered into them may be stored, used for training, or handled in ways that don't meet regulatory standards.

For any organization where client data carries legal, regulatory, or fiduciary weight, the standard consumer AI model creates unacceptable exposure. Pensato's architecture is designed to support SOC 2 compliance, CCPA obligations, and the audit requirements of FINRA, RESPA, and state bar regulations — with every data handling action logged and available for review.

Our Approach to Protecting Sensitive Data

We apply strict controls before any information ever reaches an AI model. Depending on your policies and the sensitivity of the data, we take one of three actions:



Replace

Sensitive information is swapped with temporary placeholders before it ever leaves your environment. When the AI response returns, the original values are restored internally. The AI model never sees real client or transaction data.



Remove

If certain sensitive details aren't required to answer the question, they are removed entirely. The request proceeds — the sensitive data does not.



Block

If a request contains information that should never be transmitted under any circumstances, it is stopped immediately. No data leaves your system. All blocked requests are logged for compliance review.

Full Auditability

Every action — replace, remove, or block — is recorded in an auditable format.

Your compliance and security teams have complete visibility into how data is handled at every step.