keepnet

AI + DATA SECURITY FAQ

Answers to the most common questions from CISOs, Security Architects and Privacy Officers

Does the AI ever receive or process PII?

No. All PII stays inside the Keepnet tenant. The Data Minimizer Engine strips identity fields before any AI request.

Where is customer data stored?

All data remains in the customer's selected Microsoft Azure region.

Does OpenAI retain or train on our data?

No. OpenAI Enterprise models do not train on or retain customer data.

What does the AI actually see?

Only anonymized behavioral attributes such as training history, simulation outcomes, reporting behavior, role, region, language and culture.

How is data protected at rest and in transit?

Encrypted in transit with TLS 1.2+ and encrypted at rest with AES-256.

How do you prevent unsafe or inaccurate outputs?

We use a multi-layer safety system:

- Retrieval-Augmented Generation (RAG) ensures the AI only uses verified and accurate knowledge sources
- Cloudflare AI Gateway filters all prompts and responses
- Keepnet validation layers apply safety scoring, cultural alignment, bias detection, and accessibility checks
- Optional human approval workflow for sensitive content
- Continuous monitoring for quality and correctness

Can we enforce our own AI policies?

Yes. Model whitelisting, approval workflows and access controls can be aligned to your governance rules.

What if AI produces incorrect or risky content?

All outputs pass through Cloudflare Gateway and Keepnet's validation layers. Human approval can be required.

Is customer data shared with third parties?

No customer PII is shared. Subprocessor transparency is available in the compliance portal.

How do you handle incident response?

24/7 monitoring with P1 notifications within 15 minutes. Breach notifications follow GDPR, UK DPA, CCPA and regional regulations.

Are you aligned with AI governance standards?

Yes. Keepnet operates under ISO/IEC 42001 principles and ISO 27001 certified controls.

Where can we download compliance documents?

All documents are available at:

https://doc.keepnetlabs.com/resources/compliance

Keepnet ensures enterprise-grade AI governance, data protection and operational transparency across all deployments.