AI GOVERNANCE & DATA SECURITY

Enterprise Controls · Regulatory Compliance · Third-Party Risk Management

Keepnet's Agentic AI operates under ISO/IEC 42001:2023 (AI Management Systems), ISO 27001:2022 (Information Security), and SOC 2 Type II controls with zero PII transmission, regional data residency, and contractual SLAs for breach notification, incident response, and right-to-audit.

1. Regulatory Compliance Framework

AI Governance

- ISO/IEC 42001:2023
- EU AI Act (Medium Risk)
- NIST AI RMF aligned

Data Protection (Global)

- GDPR (Art. 22, 35 DPIA)
- CCPA/CPRA, UK DPA
- APAC PDPA, LGPD aligned

Security Standards

- ISO 27001:2022 (Cert: Dec 2024)
- SOC 2 Type II (Annual)
- NIS2 Directive aligned

2. Zero-PII Architecture

✓ AI RECEIVES (ANONYMIZED)

Role category, seniority level, department function, behavioral risk score, training completion rate, simulation performance, region code, language preference

× NEVER TRANSMITTED TO AI

Name, email address, employee ID, phone number, IP address, username, location data, biometric identifiers, any GDPR Article 9 special categories

Technical Implementation:

Data minimization gateway strips all PII before any AI processing. Zero PII reaches Cloudflare AI Gateway or LLM models. Uploaded content (policy documents, training materials) undergoes same PII stripping + encryption at rest (AES-256). Prompts undergo SHA-256 hashing for audit trails. Azure OpenAI Service configured with zero retention, zero training (Enterprise tier, contractual guarantee). Cloudflare AI Gateway enforces additional guardrails for content safety and policy compliance.

3. Infrastructure

Microsoft Azure (SOC 1/2/3, ISO 27001/27018)

- Encrypted compute (AES-256)
- Hardware Security Modules (HSM)
- Network segmentation (zero-trust)
- TLS 1.3 for all transit

Cloudflare AI Gateway

- Prompt sanitization (XSS, injection)
- Output content filtering
- Rate limiting & DDoS protection
- Real-time anomaly detection

4. Data Residency

Customer-controlled regional deployment

- US: Azure Central US, East US 2
- UK: Azure UK-West, UK-South

Zero cross-border data transfer:

All processing (AI inference, storage, backups) occurs within selected region. SCCs in place for EU/UK. GDPR Article 44-50 compliant.

5. AI Model Governance & Third-Party Risk

Model Lineage & Traceability

- Azure OpenAI GPT-4o (primary)
- Azure OpenAI GPT-4-turbo (fallback)
- Cloudflare Workers AI
- Version pinning + change log
- Inference reproducibility tracked

Safety & Adversarial Testing

- Output toxicity scoring
- Hallucination detection (fact-check)
- Adversarial robustness (quarterly)
- Bias testing (quarterly)
- Human review queue (optional)

Third-Party Risk Register

Subprocessors: Azure, Cloudflare
Monitoring: Continuous risk inventory
SLA compliance: Tracked quarterly
Full list: doc.keepnetlabs.com

6. Incident Response & Contractual SLAs

Breach Notification

GDPR/NIS2: 72 hours
Keepnet SLA: 24 hours
Notification to: CISO, DPO, Legal

RTO/RPO

RTO: 4 hours
RPO: 15 minutes
Uptime SLA: 99.9%

Incident Classification

P1: 15 min response
P2: 1 hour response
P3: 4 hour response

Post-Incident

Root cause analysis (48h)
Remediation plan (72h)
Executive briefing
Lessons learned doc

7. Audit & Verification

Right to audit: On-site or remote (annual)
Audit logs: 7-year retention, immutable
Pen testing: Continuous testing by external companies
Red team: Annual (independent firm)
Bug bounty: Active program (live)
SIEM integration: Real-time log export

8. Data Lifecycle

Retention: Audit logs (7 years), configurable options available
GDPR Art. 17 (erasure): 30-day SLA
Backup deletion: 60-day cycle
Certificate of destruction: Provided upon request
Offboarding: Data export (CSV/JSON) + purge
Subprocessors: Azure, Cloudflare (full list: doc.keepnetlabs.com)

9. Insurance & Liability

D&O Insurance:
£1M coverage for management decisions

Corporate Liability:
Contract defense, crisis costs, identity fraud, investigations

Liability Cap:
12 months fees or £1M (whichever higher, standard SaaS terms)

Indemnification:
Management liability, wrongful acts, defense costs