

Security Assurance and Architecture Summary

The technical and organisational measures behind AirGap Keeper's offline, air-gapped AI processing service - written for compliance and security reviewers.

Document	Security Assurance and Architecture Summary
Audience	Compliance directors, security reviewers, instructing solicitors
Processor status	UK GDPR Article 28 processor
Facility	Access-controlled, UK-based
Data residency	UK only - data never crosses borders
Retention	Zero-retention; cryptographic erasure to NIST SP 800-88 Rev. 1 within 72 hours of completion

1. Purpose and Scope

This summary describes the technical and organisational measures AirGap Keeper applies when processing client documents and evidence media. It is written for compliance directors, information security reviewers and instructing solicitors who must satisfy themselves that processing is lawful, isolated and auditable.

It covers our physical infrastructure, media intake, model execution, data lifecycle and the assurances we give under UK GDPR Articles 28 and 32. It does not replace the Data Processing Agreement, which remains the contractual source of truth.

2. Air-Gapped Architecture

Our AI enclave runs on dedicated multi-GPU hardware with all wireless and wired networking removed or permanently disabled. There is no network interface for an attacker to reach, and no route by which client data can leave the enclave electronically.

- No Wi-Fi, Bluetooth or Ethernet connectivity in the processing machines.
- Enclave housed in an access-controlled room within a UK facility.
- Administrative access is local, logged and limited to vetted personnel.
- No remote administration tooling of any kind is installed.

3. Media Intake and Forensic Write-Blocking

Client media is received against a chain of custody reference issued before despatch. Every drive is mounted through a dedicated forensic hardware write-blocker, enforcing a physical one-way data flow so that original evidence cannot be altered during ingestion.

- Chain of custody reference issued before any media is accepted.
- Hardware write-blockers used for all read operations from client media.
- Cryptographic hashes recorded at intake and verified before return.
- Incoming PDFs are flattened in a staging environment to strip macros, embedded JavaScript and tracking pixels.

4. Local Model Execution

All analysis is performed by open-weight models running entirely on local hardware. No prompt, document, extract or embedding is transmitted to a third-party model provider, because the enclave has no means of transmitting anything at all.

Model weights are obtained once, verified by hash, and transferred into the enclave through the same controlled intake path used for client media.

5. Data Lifecycle and Chain of Custody

Client data exists in our environment only for as long as the instructed work requires. Each stage is recorded against the chain of custody reference so the full lifecycle can be reconstructed during an audit.

- Intake: media logged, hashed, write-blocked and assigned to a matter.
- Processing: analysis performed inside the enclave; working copies remain on enclave storage.
- Delivery: outputs written to client-supplied or newly issued encrypted media and despatched by tracked courier.

- Erasure: enclave working copies are cryptographically erased to NIST SP 800-88 Rev. 1 once delivery is confirmed, and a certificate of erasure is issued on request.

6. UK GDPR Articles 28 and 32

AirGap Keeper acts as a processor. We process personal data only on documented instructions from the controller, impose confidentiality obligations on all personnel, assist with data subject rights and security obligations, and delete working copies at the end of the engagement.

Our Article 32 measures include physical isolation, encryption of data at rest on all transport and enclave media, strict access control, integrity verification through hashing, and a documented restoration and incident process.

7. Physical and Personnel Controls

The facility is access-controlled, with entry restricted to named, vetted personnel. Media in transit is encrypted, and keys are exchanged through a channel separate from the media itself. Personnel are bound by written confidentiality undertakings and receive role-specific handling training.

8. Zero-Retention Assurance

We retain no client documents, extracts, embeddings, indexes or model fine-tunes after an engagement closes. Nothing derived from client data is used to train or adapt models. Business records that remain are limited to matter metadata required for accounting and audit purposes.

9. Audit and Contact

Controllers may request an audit of these measures under the Data Processing Agreement. We accommodate reasonable on-site inspections of the facility and its procedures, subject to scheduling and confidentiality arrangements.

Questions about this summary should be directed to compliance@airgapkeeper.com.

This document is provided for assurance purposes and does not constitute legal advice. The Data Processing Agreement governs the contractual relationship between AirGap Keeper and the controller.