Data Residency Statement

Sunbeam Control — AI Workforce Operations Platform

Issued by: Mishki Ltd trading as Sunbeam Control
Version: 1.0
Date: March 2026
Contact: legal@sunbeamcontrol.com

This statement describes where data created and processed by Sunbeam Control resides at every stage of the product lifecycle. It is provided for enterprise procurement, information security, and legal teams evaluating Sunbeam for deployment.

1. Core Principle

Sunbeam Control is designed on a local-first architecture. Scan findings are created on the Customer's own infrastructure and do not leave the Customer's environment unless the Customer explicitly configures an integration to send them elsewhere.

Sunbeam operates no cloud backend that receives scan data. There is no Sunbeam SaaS data pipeline. There are no Sunbeam servers in any jurisdiction that receive, store, or process Customer findings.

2. Data Residency by Configuration

Configuration	Data Location	Sunbeam Access
Standalone scanner (macOS app or CLI)	Scanned machine only — RAM during scan, output file if saved	None
CLI with --output FILE	Customer-designated file path on scanned machine	None
CLI with --webhook URL	Customer-designated HTTP endpoint	None — Customer configures destination
CLI with --splunk-url	Customer's Splunk instance	None — Customer configures destination
CLI with --slack-webhook	Customer's Slack workspace	None — Customer configures destination
Central Server (v2.5.0+)	Customer's self-hosted server — SQLite on Customer infrastructure	None
PDF / CSV report	Customer's local filesystem	None

3. No Data Leaves the Customer Environment Unless Configured

In the default product configuration (standalone scanner, macOS app), no data leaves the machine being scanned. The following components of Sunbeam do not make outbound connections carrying Customer data:

- The network scanner (scans inbound, does not transmit findings outbound)
- The workstation scanner (reads local files, does not transmit)
- The egress scanner (observes outbound connections, does not create them)
- The cloud scanner (reads cloud APIs using Customer-provided credentials, does not transmit findings to Sunbeam)
- The PDF and CSV report generator (writes locally, does not upload)
- The licence validator (validates locally in v2.x — no phone-home)

The only outbound connections made by Sunbeam are:

- Version check: a GET request to the Sunbeam R2 bucket to check if a newer version is available. This request contains no Customer data — only the request itself.
- Fingerprint update: a GET request to retrieve updated AI fingerprints. This request contains no Customer data.
- Customer-configured integrations: webhook, Splunk, Slack — only when explicitly configured by the Customer using a CLI flag.

4. Central Server Data Residency (v2.5.0+)

The Central Server is a self-hosted component deployed by the Customer on the Customer's own infrastructure. The Customer chooses the deployment environment:

- On-premises server — data remains within the Customer's physical premises
- Private cloud (AWS, Azure, GCP) — data remains in the Customer's cloud tenancy, in the region selected by the Customer
- Hybrid — combination of the above

Sunbeam does not provide or operate the Central Server infrastructure. The Customer deploys it via Docker Compose. All data stored in the Central Server SQLite database is under the Customer's control and in the Customer's chosen jurisdiction.

5. Jurisdictional Statement

Because Sunbeam does not operate a cloud backend that receives Customer data, there is no Sunbeam data processing jurisdiction to declare. Customer data remains in whichever jurisdiction the Customer's infrastructure is located.

Mishki Ltd is incorporated in England and Wales. The Sunbeam product and its update infrastructure (version.json and fingerprints.json) are served from Cloudflare R2 (European region). No Customer scan data passes through this infrastructure.

6. For GDPR-Regulated Organisations

Sunbeam's local-first architecture is designed to be GDPR-compatible by default:

- No cross-border transfer of personal data to Sunbeam — not applicable in standard configuration

- Data minimisation: only AI-relevant signals are recorded; credentials, file contents, and communications are not collected
- Purpose limitation: findings are used only for the AI workforce management purpose defined by the Customer
- Data subject attribution: OS usernames are recorded to enable the Customer to identify the owner of each agent; values of credentials are never recorded

For GDPR data protection enquiries: legal@sunbeamcontrol.com