SECURITY, COMPLIANCE & TRUST

Security is the architecture, not a feature.

How Fisar protects the data it handles — and proves it.

Fisar processes some of the most sensitive information an organisation holds: personal data pulled from across your systems, much of it concerning people other than the requester. We treat security as the foundation everything else is built on, not a feature added at the end.

Every stage of a Subject Access Request — from the moment it's logged to the moment the response is delivered and the working data is destroyed — happens inside one protected environment, in the UK, under access controls you set. This document explains three things: where your data lives, how it's protected, and how compliance is proven rather than promised.

TRUST AT A GLANCE

UK data residency

AWS London (eu-west-2). Data stays within UK borders.

Encrypted everywhere

AES-256 at rest · TLS 1.3 in transit.

Least-privilege access

Role-based permissions, protected by MFA.

GDPR Article 28

Processor agreement in place.

7-year audit trail

Every operation logged and retained.

ISO/IEC 27001

Aligned with controls · certification in progress.

01

THE PROTECTED ENVIRONMENT

Where your data lives, and who can reach it.

One protected environment in the UK — built for containment and permissioned, one-way access.

Data never leaves the UK.

All processing runs in the AWS London region (eu-west-2). Application servers sit in private network segments with no direct route to the internet; databases live in isolated, encrypted subnets.[1]

Encrypted everywhere.

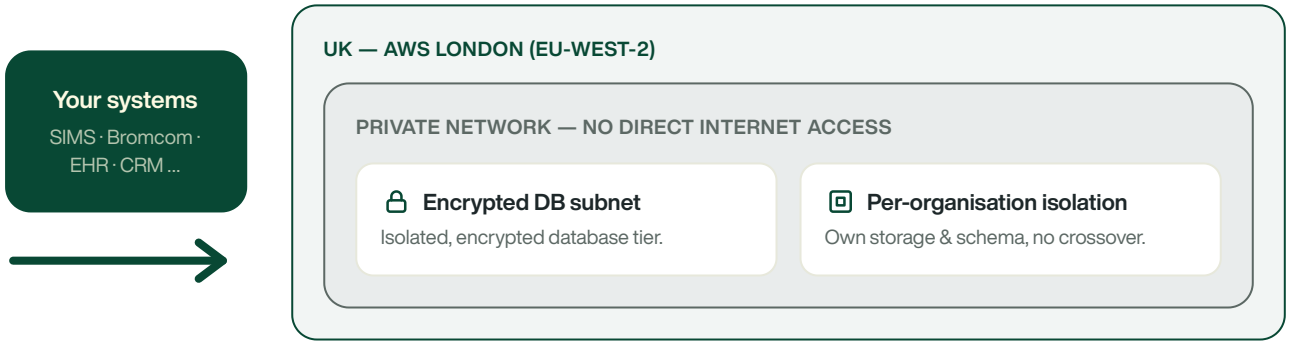
AES-256 with managed key rotation at rest, TLS 1.3 in transit.[2] Each organisation's data is kept in its own isolated storage and schema — no crossover between customers, ever.

You hold the keys.

Fisar reads from your systems only with credentials your administrators grant — and can revoke at any time. Access is role-based and protected by multi-factor authentication.

LAYERED ENVIRONMENT

read-only · credentialed · revocable



Data is protected at every layer: UK region → private network → isolated, encrypted database. Access in is one-way, read-only and permissioned. Diagram to be revisited.

ROLE	TYPICAL SCOPE	MFA REQUIRED
Trust / group administrator	Organisation-wide configuration	
Site administrator	Their own site / location	
Data Protection Officer (DPO)	Full case review & release authority	
SAR processor	Day-to-day request handling	

1 *Network architecture:* application tier runs in private subnets with no inbound internet path; database tier sits in separate isolated subnets with encryption enforced at the storage layer.

2 *Encryption:* AES-256 at rest with managed key rotation; TLS 1.3 for all data in transit. Per-tenant logical isolation at both the storage and database-schema level.

02

COMPLIANCE BY DESIGN

Proof of compliance, not just a promise.

Compliance isn't a filed-away policy — it's built into how the system behaves on every request.

Built around regulation.

A GDPR Article 28 processor agreement, designed around UK GDPR and the DPA 2018. Data minimisation is enforced automatically; breach-notification obligations are supported.[3]

A tamper-evident record.

Fisar fingerprints every operation — each retrieval, redaction and human decision — chained into one record. Alter the history and it breaks, producing a signed certificate of what happened.[4]

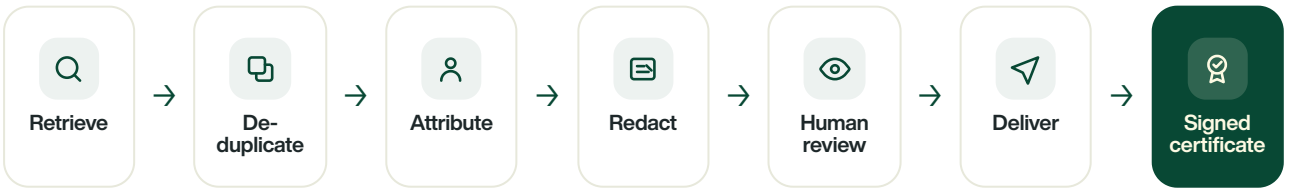
Then it cleans up.

Working copies of personal data are destroyed 30 days after a case closes, with deletion certificates kept as proof. Audit trails are retained for seven years; source systems are only ever read from.

OBLIGATION	HOW FISAR MEETS IT
Lawful basis to process (Art. 28)	Processor agreement in place
Data minimisation	Scope & date-range enforced automatically
Storage limitation	Working data auto-deleted at case close + 30 days
Accountability / audit	Tamper-evident log, retained 7 years
Breach readiness	Notification support built in
Information security	Aligned with ISO/IEC 27001 controls (cert. in progress)

CHAIN OF PROOF

tamper-evident — change one link, the chain breaks



Each operation carries its own cryptographic fingerprint, chained into a single signed certificate.

3 *Frameworks:* aligned with UK GDPR, the Data Protection Act 2018, and ISO/IEC 27001 controls (certification in progress). GDPR Article 28 processor agreement provided.

4 *The audit record:* every operation is hashed (SHA-3) into a Merkle tree whose single root fingerprint represents the entire process. The root is signed with CRYSTALS-Dilithium — the NIST-standardised post-quantum signature scheme — and stored in a write-once, immutable ledger.

03

CONNECTING SAFELY

Plugs into the systems you already use.

Scoped, read-only connections you control, and onboarding that always starts in a safe sandbox.

Vendor-approved connections.

Fisar connects through each platform's official integration route — scoped, read-only access your administrators control and can withdraw at any time. It never writes back to your systems.

Sandbox-first onboarding.

Every new connection starts with dummy data in an isolated environment, so you can see exactly how Fisar behaves before it ever touches live information.

Sector-agnostic by design.

The same secure pipeline serves education, healthcare, financial services and government — any organisation that receives Subject Access Requests.

EXAMPLE CONNECTORS

SIMS	Bromcom	Arbor	CPOMS	RM Integris
ScholarPack	Pupil Asset	iSAMS	Raptor	+ more via API

Official, vendor-approved, read-only connections — controlled by your administrators.

SANDBOX-FIRST ONBOARDING

1. Connect in sandbox (dummy data)
2. Review behaviour & permissions
3. Go live, read-only

SEE IT ON YOUR OWN TERMS

In a sandbox, with dummy data, before anything goes live.

FISAR

Book a demonstration →

Fisar is a Cybix AI product · All data processed in AWS UK (London) · fisar.co.uk