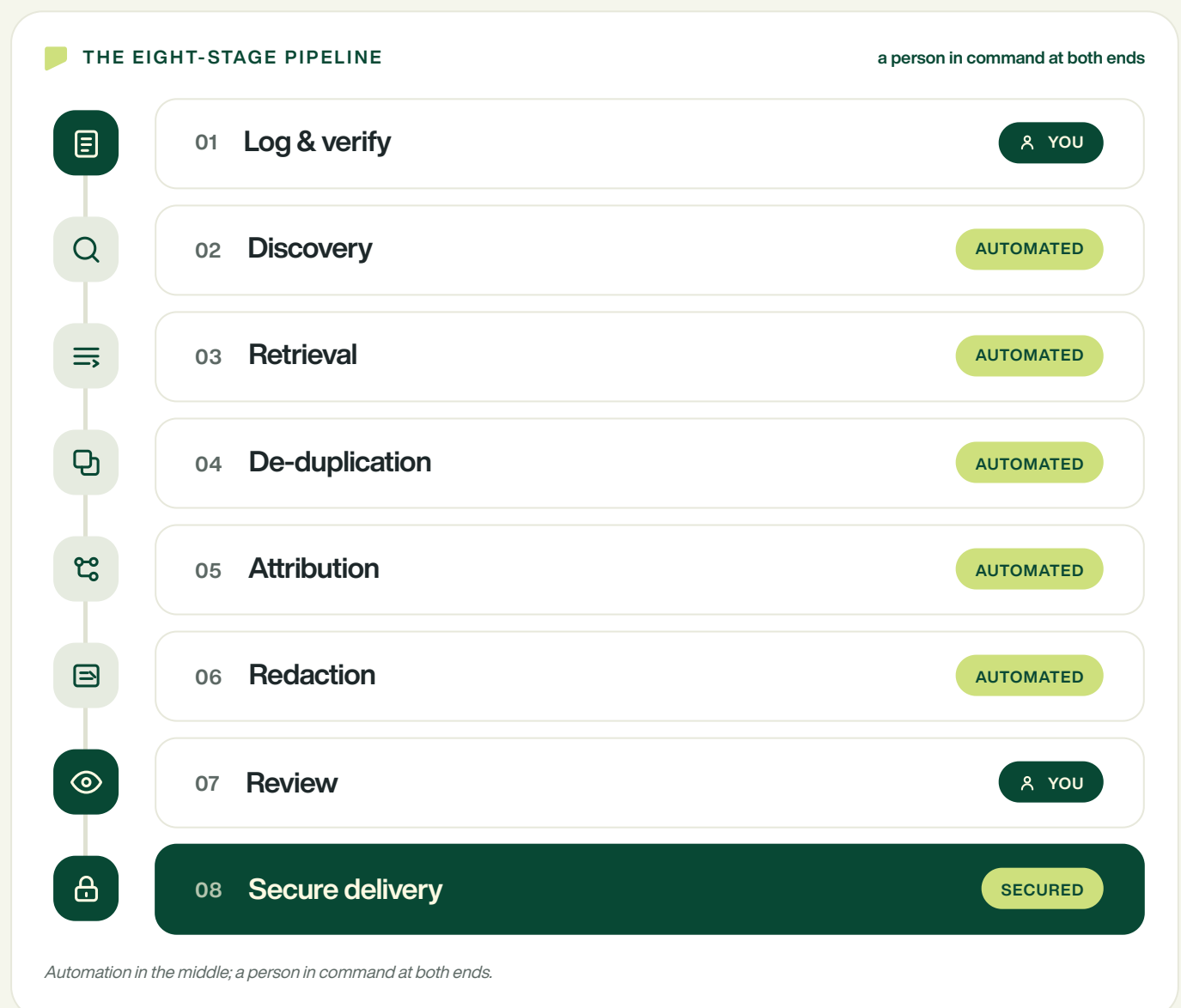


From first request to final response.

A look under the bonnet — the eight-stage pipeline, stage by stage.

Every request follows the same controlled route. A person stays in command at the start and the end; intelligent automation does the heavy lifting in between — querying systems, removing duplicates, working out whose data is whose, and proposing redactions for your team to approve. The result is faster handling without surrendering judgement.





STAGES 01-03

Logged, located, retrieved.

The front of the pipeline: a request is captured, its sources mapped, and the data collected.

01 · Log & verify

The request is logged in minutes — who is asking, on whose behalf, what data and over what date range. Before anything is collected, Fisar guides identity verification, and the statutory clock starts automatically with a live, shared status.¹

02 · Discovery & mapping

Personal data rarely sits in one place. Fisar scans every connected system to find which ones actually hold data about the requester, classifies what it finds by sensitivity, and builds a collection plan — all in read-only mode.

03 · Parallel retrieval

Instead of working through systems one by one, Fisar queries them all at once, so total collection time is set by the slowest source — not the sum of them. Data arriving in different shapes is normalised into one structure.²

PARALLEL VS. SEQUENTIAL RETRIEVAL

collection time = the slowest source, not the sum

Sequential

one system after another

SIMS

CPOMS

Email

Files

Archive

Parallel — Fisar

all sources at once

all sources

Time saved

start

elapsed time →

¹ The 30-day due date is computed from the recorded date of receipt, with escalating alerts. Identity-verification documents are checked, the outcome recorded, and the documents destroyed immediately afterwards.

² *Parallel Distributed Retrieval (PaDR)* runs up to 50 concurrent workers per request, fault-isolated per source. It learns each system's typical response time, sets timeouts at ~95% confidence, and retries slow sources with exponential backoff.



STAGES 04-06

The intelligent core.

Telling the requester's own data apart from everyone else's — the part a SAR lives or dies on.

The heart of a SAR is separating the requester's own data — which must be disclosed — from other people's, which must be protected. Simple tools match on names and fail the moment a record says "his teacher" or "the visitor she signed in with". Fisar reads documents in context instead.

04 · De-duplication

The same email forwarded around, a letter saved in three folders, a screenshot of a message — compiled blindly, these bloat the response and double the review. Fisar removes duplicates intelligently, keeping the best copy so reviewers see each item once.³

05 · Attribution

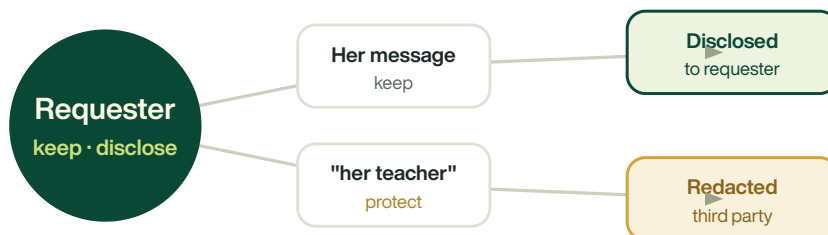
Fisar identifies every person and reference in a document, maps the relationships between them, and decides item by item whether each belongs to the requester or a third party — working across text, images, audio and video, not just names.⁴

06 · Redaction

Crude redaction destroys meaning. Rather than black-barring everything, Fisar picks the right protection for each item — masking a face, replacing a name with [TEACHER], or removing a section entirely — and routes anything high-risk to a human.

WHOSE DATA IS WHOSE?

context-aware attribution



● Requester's data — keep & disclose ● Third-party data — protect & redact

³ *De-duplication* works in three escalating levels: exact matching (SHA-256) for identical files, perceptual matching (pHash, SimHash) for near-copies like rescans, and semantic matching using embeddings to catch paraphrased or reformatted content.

⁴ *Attribution* uses a 3-layer graph neural network trained on 50,000 expert-labelled SAR documents. Redaction applies four graduated levels — mask, replace, remove, pseudonymise — driven by a risk score; critical or low-confidence items always escalate to a person.



STAGES 07-08

Approved, then proven.

A person approves every release; then Fisar proves exactly what happened and cleans up.

07 • Human review & approval

Fisar never sends anything out by itself. Everything lands in a review workspace where your DPO sees what was found, what was redacted, and why. The riskiest, least-certain items come first; routine material is one-click. Every redaction can be accepted, adjusted or overridden — professional judgement always wins.

08 • Secure delivery & proof

The approved response is compiled and delivered encrypted, with confirmation, well inside the deadline. Throughout, Fisar has fingerprinted every action into a tamper-evident certificate — cryptographic proof of compliance. Then it cleans up: working copies are destroyed 30 days after the case closes.⁵



Nothing is released until a DPO has reviewed and approved it.

⁵ Every operation is hashed (SHA-3) into a Merkle tree whose single root represents the whole process; the root is signed with post-quantum cryptography and stored in an immutable, write-once ledger. Audit trails are retained for seven years.

SEE THE PIPELINE LIVE

Watch a request travel all eight stages.



Book a demo

