



Trust & Security

Trust & Security · publicly shareable overview · July 2026

Strivio is built for environments where decisions and data matter. This overview brings the safeguards together in one place. The full substantiation is in the *Technical Memo (under NDA)*, the data protection note and the data processing agreement.

Data residency — entirely within the EEA

Storage, application and AI processing all take place within the European Economic Area. There is no transfer to countries outside the EEA — zero transfer points, so no additional transfer safeguards are required.

- **Storage.** Hosted within the EEA; encryption at rest on by default.
- **Application & processing.** Hosted within the EEA; stateless server components and API routes.
- **AI layer.** An AI service with a processing region within the EEA; no training on customer data.

Isolation & access

- **Strict multi-tenant isolation.** Row-Level Security at database level: each organisation sees only its own runs, snapshots and feedback.
- **Role-based access.** Authenticated users only, roles separated (user/admin), following least privilege.
- **Key management.** Privileged keys are used server-side only, never in the browser.

AI with guardrails — no fabricated outcomes

- **Closed reference set (RAG).** The model selects and re-ranks only from a shortlist of real, existing portfolio items; it cannot generate non-existent items. Where coverage is missing, Strivio shows it as an honest gap.
- **No training on customer data.** Customer data is not used to train or improve the underlying models.
- **Data minimisation toward the model.** Only the fragments needed for the analysis are sent.
- **Additional shielding available.** For sensitive environments, a mode can be enabled whereby prompts and responses are not stored and no human review takes place.
- **Human in the loop.** AI output is supportive and reviewed by users; no automated decision-making with legal effect.

Source, reliability & traceability

- **Read-only source connection.** Strivio reads from the portfolio tool (Azure DevOps) and does not write back into source systems unprompted; write-back happens only explicitly and labelled.
- **One source of truth.** Screen and export show the same numbers; identical input yields the same outcome.
- **Audit trail.** Access and changes are logged; per-run snapshots make decisions traceable over time.

Sub-processors — all within the EEA

Strivio works with a small number of sub-processors for database/storage, application hosting and AI processing — all hosted within the EEA, with encryption at rest and no training on customer data. The current, named sub-processor list with regions is shared on request and as part of the data processing



agreement.

The named sub-processor list (Sub-processor Annex) is available on request and under NDA; changes are notified in advance.

Governance & compliance

- **GDPR-aligned.** Processing in accordance with the GDPR; a data processing agreement (Art. 28 GDPR) and data protection note are available and reviewable by the Data Protection Officer.
- **DPIA-ready.** The processing is described and scoped so that a DPIA, where the controller deems one necessary, can be carried out directly.
- **Breach notification.** Notification to the controller without undue delay, within 48 hours of discovery at the latest.
- **Deletion or return.** After a pilot ends or on first request, all data is deleted or returned — including at sub-processors, with written confirmation.

Under NDA we share the Technical Memo (full architecture, matching engine and data model) and the named Sub-processor Annex. — Strivio is a trade name of Dakota Digital B.V. (Dutch CoC 88261034).