RegAlign®
Trust Pack

Prepared for procurement, information security, and legal reviewers evaluating RegAlign. This single document answers the questions a buyer typically asks in the first round of diligence. Everything stated here is either visible in the product or already covered by another canonical RegAlign document; this Trust Pack is the index.

For the live versions of every section, see the public Trust Centre at `https://regalign.app/trust`.

1. Company and registration

- Legal entity: RegAlign Limited, Jersey company No. 165263, publisher of RegAlign® and RiskAlign™.
- Jurisdiction: Jersey, Channel Islands.
- Trademark: UK00004263780 (RegAlign).
- Data protection registration: Jersey Office of the Information Commissioner (JOIC), entry on the JOIC public register.
- Public Trust Centre: `https://regalign.app/trust`
- Hash-chain verifier: `https://regalign.app/verify`
- Auditor access: `https://regalign.app/auditor-access`

2. Hosting and data residency

- Application: Cloudflare Workers (UK/EU edge regions preferred).
- Database, authentication and storage: Lovable Cloud (managed Supabase, EU region).
- All customer data is encrypted in transit (TLS 1.2+) and at rest (AES-256 at the database and storage layers).
- No customer data is held on RegAlign-owned laptops or shared file services. Operator access is browser-only and audit-logged.

3. Sub-processors

Sub-processor	Purpose	Region
Cloudflare	Edge compute, CDN, DDoS protection	Global
Lovable Cloud	Database, authentication, storage	EU
Google Cloud	AI Gateway (LLM inference)	EU
Resend	Transactional email	EU

The list above is canonical. Material changes are notified by email to each tenant's primary contact at least 30 days before they take effect.

4. Data we collect and why

RegAlign processes only the operational data a customer chooses to load: obligations, controls, evidence, decisions, findings, and the metadata required to maintain the linkage spine between them. We do not process special-category personal data. We do not sell, share or use customer data to train any AI model.

5. Retention and deletion

- Live tenant data is retained for the duration of the agreement plus 90 days, then purged.
- Append-only audit-trail entries and evidence hashes are retained for seven years to support regulatory replay; payload bodies are purged on the same 90-day cadence.
- A customer may request earlier deletion in writing; deletion is irreversible and is acknowledged within five working days.

6. Authentication and access control

- Multi-factor authentication is enforced on founder accounts and is available to every tenant administrator.
- Role-based access control is enforced at the database via row-level security on every public table.
- Operator session tokens are short-lived and rotated automatically; there are no long-lived static credentials.
- All privileged operations are written to the append-only audit trail and surfaced in the in-product audit-trail viewer.

7. Hash-chain and tamper-evidence

Every evidence record and every audit-trail entry is hashed with SHA-256 at the moment it is sealed. The hash is published into a public verifier (`/verify`) so any auditor, regulator or counter-party can confirm a receipt without an account and without seeing any tenant identifiers. The verifier returns only:

- whether the hash matches,
- the sealed-at timestamp,
- the evidence kind or chain position,
- an opaque tenant tag, and
- a verification reference (VR-…).

It never returns tenant names, source references, file names, user IDs or access-control metadata.

8. Business continuity

- Recovery Point Objective (RPO): 24 hours.
- Recovery Time Objective (RTO): 8 hours.
- Daily encrypted backups are taken at the database and storage layers and are tested quarterly.
- A founder runbook for full-service restoration is maintained in `docs/canonical/07_BCP_Outline.md` and rehearsed annually.

9. Security testing

- Static analysis and dependency scanning run on every change.
- An independent penetration test is scheduled before each pilot conversion and after each material architectural change. Scope is set out in `docs/canonical/08_Pen_Test_SoW.md`.

- A coordinated vulnerability-disclosure policy is published at `docs/canonical/28_Vulnerability_Disclosure_Policy.md`.

10. AI use disclosure

RegAlign uses large-language-model inference through the Lovable AI Gateway for narrowly-scoped operator-facing tasks: drafting correspondence, summarising findings, and classifying obligation applicability. The full disclosure — what we do and what we explicitly do not do — is in `docs/canonical/29_AI_Use_Disclosure.md`. Customer data is never used to train any model.

11. Certification roadmap

Item	Status
Data protection (JOIC)	Live
Hash-chain verifier	Live
Public Trust Centre	Live
Vulnerability disclosure	Live
CSA CAIQ v4 self-assessment	Live (see §11a)
Independent penetration test	Pre-conversion
CSA STAR Registry (Level 1)	Submission in progress
ISO 27001	Planned, post-pilot
SOC 2 Type I	Planned, post-pilot

11a. CSA CAIQ v4 Level 1 self-assessment

RegAlign maintains a full Consensus Assessments Initiative Questionnaire v4 self-assessment covering all 197 CCM v4 controls. Read it online at `https://regalign.app/trust/caiq` (per-question anchors for procurement RFP deep-linking) or download the PDF at `https://regalign.app/downloads/canonical/regalign-caiq-v4-level1.pdf`. The CSA STAR Registry listing will be linked here once published (expected within two weeks of CSA submission).

We do not claim a certification we do not hold. The above is the honest state of play as at the date on the cover of this document.

12. Contacts

- Security and vulnerability disclosure: `security@regalign.app`
- Data protection: `dpo@regalign.app`
- General trust queries: `trust@regalign.app`

A named individual will reply within two working days.