RegAlign®

Data Protection Impact Assessment — Template

Status: Canonical Data Protection Impact Assessment template. Completed per-customer, retained by RegAlign and provided to customer's DPO/MLRO on request. **Aligned to:** Data Protection (Jersey) Law 2018 (DPJL) and the Data Protection Authority (Jersey) Law 2018 (DPAJL), with guidance from the Jersey Office of the Information Commissioner's DPIA guidance. **Owner:** Sabrina Stewart.

How to use

- 1. Open this template and save as `DPIA_[Customer]_[YYYYMMDD].docx` in `/docs/canonical/dpias/`.
- 2. Complete every section. Mark "Not applicable" with reason — never blank.
- 3. Review with customer's DPO / MLRO before pilot go-live.
- 4. Refresh annually or on material change (new jurisdiction, new processing purpose, new sub-processor).

---

1. Processing overview

- **Customer (Controller):** [Name, JFSC registration number]
- **Processor:** RegAlign Limited (Jersey company no. 165263, registered office 9 Bond Street, St. Helier, JE2 3NP). RegAlign® is a registered UK trade mark, UK00004283882, owned by Sabrina Stewart and licensed to RegAlign Limited.
- **Sub-processors:** Supabase (data layer, EU region), Cloudflare (edge, EU + global), [others as deployed]
- **Processing purpose:** Production, retention, and presentation of JFSC Code-of-Practice compliance evidence on behalf of the Controller.
- **Categories of data subject:** Customer's own clients (natural persons), beneficial owners, PEPs, settlors, trustees, directors, controllers, Customer's own staff (users of the platform).
- **Categories of personal data:** Identification data, contact data, identification document references, sanctions/PEP screening results, source-of-funds narrative, transaction summaries (where uploaded), compliance assessments, board minutes references.
- **Special category data:** Only where Customer uploads — e.g. health data referenced in vulnerability assessments. Documented per upload.
- **Legal basis (Controller's):** Legal obligation (AML/CFT regulation), Legitimate interest (governance), Contract (client engagement).
- **Legal basis for RegAlign's processing:** Contract with Controller.

1a. Access-control and audit processing (RegAlign as Controller)

Separately from the customer-data processing above, RegAlign Limited acts as **Data Controller** in its own right for the small set of personal data it collects to operate the platform's access wall. This is recorded here so the customer's DPO can see the full picture in a single document.

- **Purpose:** Invite-only access control and audit of platform use.
- **Data subjects:** Prospective users who submit `/request-access`; invited users who hold an account.

- **Categories:** Name, work email, firm, role/title, free-text reason; IP address and browser user-agent at submission; sign-in / sign-out timestamps; hashed password (never plain text).
- **Lawful basis:** Legitimate interests (controlling access to a regulated tooling environment and maintaining an audit trail). For invited pilot participants this is also performance of contract.
- **Retention:** Access-request records — 24 months from submission, or earlier on request. Authentication audit logs — ~7 days. Account profile — life of account plus reasonable audit residue. See `15_Data_Retention_and_Deletion.md`.
- **Recipients:** RegAlign Limited founder mailbox (for triage) via the transactional email queue. No onward disclosure.
- **Cross-border transfer:** None beyond the EU-resident Supabase region and Cloudflare edge already disclosed in `14_Sub_Processor_List.md`.
- **Regulator registration:** RegAlign Limited is registered with the Jersey Office of the Information Commissioner as a controller and processor under the Data Protection Authority (Jersey) Law 2018 (DPAJL), Registry No. **103914** (verifiable at https://jerseyoic.org/Registrations/RegistrySearch/Index).

2. Necessity and proportionality

- Why is RegAlign needed? [Customer-specific: e.g. demonstrating COP compliance at board level without manual evidence assembly.]
- Could the purpose be achieved with less data? [Assessment: e.g. no, because COP evidence chain requires linkage between identification, screening, decision, and approval records.]
- Retention: customer-controlled retention policy applied per data category. Default 7 years post-relationship end (aligns to JFSC handbook expectation).
- Data minimisation: RegAlign does not request data beyond what Controller uploads. No enrichment or profiling beyond what Controller configures.

3. Data flows

- **Ingress:** Web UI (TLS 1.3), authenticated session, customer's own users.
- **At rest:** EU-region database, AES-256 encryption at rest, RLS-enforced tenant isolation.
- **In transit:** TLS 1.3 for all customer-facing traffic; mTLS for inter-service where applicable.
- **Egress:** Customer-initiated export only; no third-party data sharing without customer's written instruction.
- **Backups:** EU region, encrypted, retention [period], tested [frequency].
- **Sub-processor list:** Maintained at `/docs/canonical/sub-processors.md`, customer notified 30 days before any change.

4. Risks identified

Risk	Likelihood	Severity	Mitigation	Residual
Cross-tenant data leak via RLS misconfiguration	Low	High	RLS policies covered by integration tests; every migration reviewed against policy set; quarterly access review	Low

Risk	Likelihood	Severity	Mitigation	Residual
Sub-processor outage (Supabase / Cloudflare)	Low–Medium	Medium	BCP per `07_BCP_Outline`; customer-initiated data export available; documented recovery time objective	Medium
Unauthorised access via compromised customer user credential	Medium	High	Enforced MFA available; session timeout; access log review; IP allow-listing optional	Medium
Single-founder key-person event	Medium	Medium–High	Source-code escrow available to customers requiring it; documented runbooks; designated technical advisor on retainer (in progress)	Medium
Data subject rights request (access, rectification, erasure)	Medium	Low–Medium	Customer-initiated workflow in product; RegAlign assists Controller within 5 business days	Low
Regulatory request for data disclosure	Low	High	Customer notified unless legally prohibited; legal review before any disclosure	Low
Pen-test gaps / undiscovered vulnerabilities	Medium	Medium–High	Annual pen test (see `08_Pen_Test_SoW`); responsible-disclosure process; vulnerability log	Medium

5. Data subject rights handling

- **Right of access:** Customer-initiated within product; RegAlign assists within 5 business days.
- **Right of rectification:** Customer self-serve within product.
- **Right of erasure:** Customer self-serve, subject to Controller's retention obligations (Customer's call, not RegAlign's).
- **Right to restrict processing:** Per-record flag available; RegAlign-side honoured by suppression from active workflows.
- **Right to data portability:** Machine-readable export available on request.
- **Right to object:** Routed to Controller; RegAlign has no independent processing decision-making.

6. International transfers

- Primary hosting: EU region (Supabase EU).
- Edge / CDN: Cloudflare global. Personal data not cached at edge; only static assets.
- Any non-EU transfer requires explicit customer notification and a documented transfer mechanism (SCC equivalent or Jersey-recognised adequacy).

7. Sub-processor register (snapshot — full list maintained separately)

Sub-processor	Purpose	Region	Transfer mechanism
Supabase	Database, auth, storage	EU (Frankfurt)	Intra-EEA
Cloudflare	Edge, DNS, CDN	Global (no PII cached)	Transfer mechanism documented per region
[Others as added]			

8. Consultation

- Customer DPO / MLRO reviewed: [Date, Name]
- Customer-side approval to proceed: [Date]
- Jersey OIC consultation required? [Y/N, with reasoning]

9. Sign-off

- RegAlign (Sabrina Stewart, founder): [Date, signature]
- Customer DPO / MLRO: [Date, signature]
- Review date: [Annually, or on material change]

10. Change log

Date	Change	Approved by
[Initial]	First version completed	