RegAlign®

Business Continuity Plan — Outline

Status: Canonical BCP outline. Single-founder reality acknowledged honestly. Refreshed quarterly. **Owner:** Sabrina Stewart. **Linked to:** `06_DPIA_Template`, `08_Pen_Test_SoW`.

Scope

Continuity of RegAlign service and customer-data integrity in the event of:

- Infrastructure outage (sub-processor failure).
- Cyber incident (intrusion, ransomware, denial of service).
- Founder unavailability (illness, accident, death).
- Regulatory or legal compulsion affecting RegAlign operations.

This document is honest about single-founder constraints. It does not claim resilience that does not exist; it documents what exists and what compensating controls customers can rely on.

Recovery objectives (current state)

Scenario	RTO (Recovery Time Objective)	RPO (Recovery Point Objective)	Confidence
Sub-processor outage (Supabase region)	8 hours	1 hour	Medium — depends on Supabase recovery
Application-layer regression	2 hours	0 (rollback)	High
Cyber incident requiring forensic isolation	24–48 hours	4 hours	Medium
Founder unavailability ≤7 days	Best-efforts (no SLA)	N/A	Honestly Low — documented runbooks, no second operator
Founder unavailability >7 days	Escrow + designated technical advisor activation	N/A	Low–Medium (in progress)

These objectives are honest as at the current single-founder stage. As RegAlign hires or contracts a second operator, these will tighten.

Data residency

Customer data (database rows and file storage) is resident in the **European Union (Ireland)** by default. Edge routing via Cloudflare is global; no payload is retained at edge beyond routing. AI gateway calls egress from EU infrastructure under no-training contractual terms. The full sub-processor list and the regions in which each operates is published in `14_Sub_Processor_List`. Per-tenant region pinning outside EU/Ireland is available on paid plans only by explicit written agreement.

Infrastructure continuity

- **Primary hosting:** Managed Postgres in EU (Ireland), operated via Lovable Cloud. Multi-AZ within region. See `14_Sub_Processor_List` for the named processor.
- **Edge:** Cloudflare global; EU-origin first byte.

- **Backups:** Daily automated database snapshot, retained 30 days, encrypted, EU region. Tested restore quarterly (first production drill scheduled within 60 days of first paying customer — see `27_Security_Roadmap`).
- **Source code:** Git, multiple remotes (GitHub primary, secondary mirror).
- **Secrets:** Stored in Lovable Cloud secrets vault; copy held offline in encrypted founder-controlled vault.
- **Infrastructure-as-code:** Database migrations versioned in repo (135+ migrations as at this version); platform configuration documented.

Cyber-incident response

- 1. **Detect** — monitoring alerts, customer report, or third-party notification.
- 2. **Contain** — revoke compromised credentials, isolate affected services, preserve forensic data.
- 3. **Assess** — scope of data affected, regulatory notification triggers (JOIC, JFSC, customer DPOs), legal review.
- 4. **Notify** — affected customers within 72 hours of confirmed personal-data breach, regulator per Jersey DP Law timeline, public statement if material.
- 5. **Recover** — restore from backup if needed, deploy patches, restore service.
- 6. **Review** — written post-incident review within 14 days, shared with affected customers, fed back into pen test scope and DPIA refresh.

Incident contact: founder direct line, backup contact [designated technical advisor — name TBC], legal contact [Jersey firm — name TBC].

Founder-unavailability protocol (key-person risk)

This is the single largest BCP risk and is documented openly to customers requiring it.

Compensating controls in place or in progress:

- **Runbooks** for deployment, rollback, secret rotation, backup restore, customer data export — maintained at `/docs/runbooks/` (to be created).
- **Designated technical advisor** on retainer — identified, signed engagement pending.
- **Source-code escrow** offered to any customer requiring it as a contract term. Provider: [TBC — Jersey or UK escrow agent].
- **Customer data portability** — every customer can self-serve machine-readable export at any time, no dependency on RegAlign availability.
- **Documented succession contact list** — held by founder's named legal contact, accessible on documented trigger.

Honest gap: No second permanent operator exists today. This is acknowledged in `01_SWOT_v2` as a weakness. Customers signing Bounded or Bespoke contracts should be told this directly. Customers requiring formal continuity guarantees beyond current state should receive source-code escrow as the compensating control.

Sub-processor dependency map

Service	Single point of failure?	Compensating control
Supabase	Yes — primary database	Daily encrypted backups in independent region; documented restore path
Cloudflare	Yes — edge	Origin reachable direct in degraded mode; DNS failover possible

Service	Single point of failure?	Compensating control
Lovable Cloud	Yes — build/deploy pipeline	Source code held independently; can be redeployed via standard TanStack tooling
Email (transactional)	No — replaceable	—

Testing and review

- **Backup restore test:** quarterly, results logged.
- **Tabletop incident exercise:** semi-annually (founder + technical advisor when engaged).
- **Pen test:** annually (see `08_Pen_Test_SoW`).
- **BCP review:** quarterly, or after any actual incident.
- **Customer-facing summary** refreshed annually and on material change.

What customers get on request

- This document (current version, redacted of internal contacts).
- DPIA template completed for their scope (`06_DPIA_Template`).
- Latest pen-test executive summary (when available).
- Sub-processor register (`/docs/canonical/sub-processors.md`).
- Insurance certificate (PI and cyber — when in place).
- Source-code escrow option (on request, customer-paid).

Honest limitations to disclose

- Single founder, single technical operator today.
- No 24/7 on-call.
- No multi-region active-active.
- No formal ISO 27001 / SOC 2 certification (planned post-funding or post-first-Bounded-deal).

These are not hidden. They are stated up-front to every Bounded and Bespoke prospect. The compensating controls above are the answer.
