**ADD-01 — DPIA & Regulatory Mapping (GDPR/CCPA + Export Controls)**

**Status:** New

**Intent**  
Document lawful basis, data flows, risks, and mitigations across Partner Store, screening, licensing — so privacy & export regulators (EU/US/IN) can see proof on demand.

**Actors**  
Privacy Lead • Security Architect • DPO/Legal • Audit Vault

**Preconditions**

* Data inventory of artifacts (Partners, Sites, KYC, CBT/LRT, snapshots, logs).
* Retention matrix (already designed) available.

**Flow (happy path)**

1. **Scope & Purposes:** map processing purposes (screening, licensing, audit) to legal bases (legitimate interest, legal obligation).
2. **Data Flow Diagrams:** for each purpose, draw system + third-party flows; mark cross-border transfers and processors.
3. **Risk Assessment:** identify risks (PII exposure, false positives) → mitigations (tokenization, minimization, redaction, consent where applicable).
4. **DPIA Report:** document outcomes, residual risks, DPO sign-off; store in Audit Vault with hash.
5. **Record of Processing Activities (ROPA):** generate ROPA entries per tenant/purpose; tie to retention & residency.
6. **Ongoing Review:** set annual review + change triggers (new dataset, new country).

**Edge Cases**

* New country/processor → mini-DPIA addendum.
* Mixed business/personal partners → separate lawful bases + UI cues.

**Done when**

* DPIA + ROPA published; residual risks approved; evidence stored (hashes, dates, signers).
* Data minimization rules tied to forms/exports and enforced.

**Deliverables**  
DPIA PDF, updated ROPA, flow diagrams, mitigation backlog items.