**OPS-16 — DSAR (Access/Export) Workflow**

**Intent**  
Respond to data-subject access/portability requests with **complete, redacted** partner data in SLA.

**Preconditions**

* PII map (which fields store personal data) and redaction rules.

**Flow**

1. **Intake**: verify requester identity; create DSAR ticket.
2. **Assemble**: collect partner data (core, sites, KYC docs, decisions, logs) respecting retention & residency.
3. **Redact**: apply policy (hide tokens/keys, mask IDs); generate **DSAR Pack** (JSON + PDFs).
4. **Deliver**: secure download with time-boxed link; log access.
5. **Close**: store DSAR receipt (hash of package, time, operator).

**Edge cases**

* Residency: build DSAR Pack within tenant region.
* Exceptions (legal holds) → inform scope limits.

**Done when**

* DSAR fulfilled within SLA; audit trail includes pack hash and access log.