OFFLOAD SECURITY

DPDP Act Compliance (India)

Module Whitepaper

A Data Fiduciary's control panel for the DPDP Act, 2023 and CERT-In Directions

Version 1.0 · July 2026 · Classification: Customer-Shareable

1. Overview

The DPDP module operationalizes India's Digital Personal Data Protection Act, 2023 and the CERT-In Directions 2022 for Data Fiduciaries: breach notification with statutory deadlines, DPIA lifecycle, Significant Data Fiduciary classification, vendor due diligence, and audit-ready evidence packs.

2. Key Capabilities

- Breach notification lifecycle per Rule 7: detect → declare → assess reportability → report → close, with deadline tracking for the Data Protection Board (72 hours) and CERT-In (6 hours), including watchdog alarms as deadlines approach.
- Rule 7(2) nine-section breach report validation and rendering; CERT-In Annexure I coverage across 18 incident categories.
- DPIA (Data Protection Impact Assessment) lifecycle: draft → review → approve / reject / expire, satisfying Section 13 obligations.
- Significant Data Fiduciary (SDF) classification scoring with the additional Section 10 obligations surfaced.
- Vendor/processor due-diligence assessments (18-question) with PASSING / CONDITIONAL PASS / FAILING outcomes.
- SCF-mapped readiness scoring with a Section 8(6) penalty-exposure estimate.
- Immutable audit-event log and generated audit packs for regulator or board review.
- Transfer impact analysis for cross-border data flows.

3. How It Works

The module is built as a pure domain core — state machines, validators, and scoring with no I/O — wrapped by orchestration services that persist state, emit audit events, and integrate with the platform risk register. This layering makes every statutory workflow deterministic and testable.

All DPDP collections are strictly team-scoped, and every material action lands in an immutable audit-event log from which audit packs are generated.

4. Data Handling & Security

Aspect	How it is handled
Credential protection	All connection credentials are encrypted at rest with Fernet authenticated encryption (AES-128-CBC + HMAC), decrypted in memory only at the moment of use, and never returned by APIs.
Tenant isolation	Every record is scoped to the owning team; all reads and writes filter on the tenant identifier, enforced by database indexes.

Aspect	How it is handled
Retention & deletion	Results are subject to configurable retention windows; data can be hard-deleted per scan and is removed by the tenant-offboarding cascade.
Deployment	Available as SaaS or fully self-hosted / on-premises — in the on-premises model no security data leaves your environment.

5. One Platform, One Risk View

DPDP readiness and breach posture feed the enterprise risk register and compliance dashboards; breach workflows can raise central platform alerts; and evidence generated here joins the same reporting layer as the rest of the platform.