DPDP Foundation Handbook

From statutory concepts to working privacy operations

Generated from the DPDP Foundation courseware · Review date: 2026-11-27

Purpose

This handbook helps teams turn DPDP obligations into owners, notices, consent records, rights workflows, safeguards, processor controls, retention decisions and evidence. It is an implementation aid. Legal applicability, organisation policy and regulator decisions require qualified review.

How to use this handbook

- Define the organisation and product scope before drafting notices or controls.
- Assign an accountable owner and evidence location for every obligation.
- Use the consent and rights journeys in the application to test real operating behaviour.
- Record unresolved questions as tasks or risks; never treat a score as a legal certificate.

Module 01 · DPDP Operating Model And Accountability

Duration: 35 min

Understand the DPDP roles, records, owners, and evidence that make a compliance program operational.

- Data Principal, Data Fiduciary, Data Processor, consent manager, Significant Data Fiduciary, and Data Protection Board roles.
- How a compliance obligation becomes a control, owner, task, workflow, evidence item, risk, and report.
- Why readiness scores are useful for prioritization but do not replace legal review or regulator decisions.
- How to create a practical scope statement by product, region, data category, system, vendor, and business process.

Lab: Draft a one-page DPDP scope statement for your organization.

Artifact: DPDP scope and ownership memo

Module 02 · Notice, Consent, Withdrawal, And Consent Evidence

Duration: 55 min

Build collection-point notices and consent evidence that are specific, versioned, withdrawable, and usable across systems.

- Notice content: personal data categories, purposes, rights route, grievance route, language, and versioning.
- Consent quality: free, specific, informed, unconditional, unambiguous, and affirmative action.
- Consent receipts: source, notice version, channel, language, purpose code, status, timestamp, and event history.
- Withdrawal propagation: downstream suppression across CRM, LOS, LMS, support, CDP, analytics, marketing, and processors.

Lab: Create a purpose catalog and consent receipt schema for one user journey.

Artifact: Notice and consent evidence pack

Module 03 · Legitimate Uses, Purpose Limitation, And Data Minimization

Duration: 40 min

Separate consent-based processing from legitimate uses, and prevent purpose drift.

- How voluntary data, employment, emergencies, legal obligations, and state-related contexts differ from broad consent.
- Purpose limitation as a product, analytics, marketing, and data warehouse control.
- Data minimization reviews for forms, APIs, uploads, event schemas, enrichment, and profiling.
- How to document non-consent processing without turning it into a shortcut around user choice.

Lab: Map one product workflow to purpose, data category, lawful basis, system, and owner.

Artifact: Purpose limitation and minimization matrix

Module 04 · Data Principal Rights, Grievance, And Nomination

Duration: 50 min

Operate access, correction, erasure, withdrawal, grievance, and nomination workflows with proof of closure.

- Rights covered by the program: access, correction, completion, updating, erasure, grievance, and nomination.
- Identity verification that is strong enough to prevent disclosure but proportionate enough to avoid overcollection.
- Request routing across support, legal, privacy, engineering, vendors, processors, and data owners.
- Closure evidence, refusal rationale, user communication, escalation, and response templates.

Lab: Create a DSAR and grievance workflow with owners, SLAs, and downstream tasks.

Artifact: Rights and grievance operating playbook

Module 05 · Retention, Deletion, Legal Holds, And Records

Duration: 45 min

Turn retention policy into system-level deletion, suppression, archive, and legal-hold operations.

- Retention rules by purpose, data category, system, processor, business need, and legal requirement.
- Lifecycle states: active use, suppression, restricted archive, legal hold, anonymization, deletion, and backup expiry.
- How deletion applies to logs, exports, support attachments, data warehouses, backups, and processor systems.
- How to prove deletion, retention exception, or purpose completion during an audit or dispute.

Lab: Build a retention and deletion control matrix for five systems.

Artifact: Retention schedule and deletion matrix

Module 06 · Security Safeguards And Breach Response

Duration: 60 min

Connect DPDP safeguards to practical security controls, breach triage, notifications, and incident evidence.

- Reasonable safeguards across encryption, MFA, access control, logging, monitoring, backups, secure SDLC, and vendor controls.
- Breach triage: nature, extent, timing, location, affected data, users, processors, impact, containment, and mitigation.
- Decision logs for notification thresholds, legal approval, executive updates, user communication, and regulator response.
- Processor escalation windows, contact validation, tabletop testing, and post-incident remediation evidence.

Lab: Run a tabletop breach exercise and complete the decision log.

Artifact: DPDP breach response runbook

Module 07 · Children, Significant Data Fiduciary, DPIA, And DPO Readiness

Duration: 50 min

Identify high-impact processing and prepare the governance layer needed for children's data and SDF-style obligations.

- Children's data: age gating, verifiable parent or guardian authorization, profiling restrictions, and harmful processing risk.
- SDF applicability signals: scale, sensitivity, systemic impact, children, rights risk, and public impact.
- DPO readiness: appointment, independence, contact publication, escalation, and leadership reporting.
- DPIA and independent review triggers for high-risk processing, new products, vendors, and sensitive contexts.

Lab: Create a children's data and SDF applicability memo.

Artifact: Children and SDF governance pack

Module 08 · Processors, Vendors, Subprocessors, And Transfers

Duration: 45 min

Build a third-party privacy program for contracts, processor instructions, subprocessor changes, transfers, and offboarding.

- Processor register: vendor, data category, purpose, country, owner, contract, DPA, risk score, and reassessment date.
- Contract clauses for processing instructions, confidentiality, safeguards, breach notice, deletion, and audit support.
- Cross-border processing: hosting region, support access, backups, subprocessors, restricted destinations, and notice impact.
- Withdrawal, correction, deletion, and breach task propagation to vendors and subprocessors.

Lab: Score three vendors and create a processor offboarding checklist.

Artifact: Vendor and processor governance pack

Module 09 · Evidence Packs, Board Reporting, And Regulator Readiness

Duration: 55 min

Assemble a defensible evidence pack and turn assessment gaps into a board-ready remediation roadmap.

- Evidence pack contents: notices, consent, rights, breach, vendors, deletion, safeguards, DPIA, training, reports, and decisions.
- Risk treatment: severity, owner, due date, residual risk, treatment plan, acceptance, and review cadence.
- Board reporting: readiness score, critical gaps, overdue tasks, evidence status, vendor risk, breach readiness, and trends.
- Regulator response: chronology, owners, exports, legal review, source records, and communication control.

Lab: Generate a 30-day remediation roadmap from assessment gaps.

Artifact: Board-ready DPDP status report

Statutory reference topics

- Key timelines and deadlines: Detailed breach report to the Board — Within 72 hours of discovery (R.7)
- Key timelines and deadlines: Notify affected Data Principals of a breach — Without delay on breach awareness (R.7 / S.8)
- Key timelines and deadlines: Pre-erasure notice to Data Principals — 48 hours before scheduled erasure (R.8)
- Key timelines and deadlines: Respond to a rights request — Within 90 days (maximum) (R.14)
- Key timelines and deadlines: Appeal a Board order to TDSAT — Within 60 days of the order (S.22)
- Key timelines and deadlines: Security and access log retention — Minimum 1 year (R.6)
- Key timelines and deadlines: Consent Manager audit-trail retention — Minimum 7 years (R.4)
- Key timelines and deadlines: Consent Manager regime effective — November 2026 (R.4)
- Penalty schedule: Failure to implement security safeguards — Up to ¹250 crore (S.
- Penalty schedule: Breach of children's-data obligations — Up to ¹200 crore (S.21)
- Penalty schedule: Failure to notify a data breach — Up to ¹200 crore (S.21)
- Penalty schedule: Breach of additional SDF obligations — Up to ¹150 crore (S.21)
- Penalty schedule: Other violations — Up to ¹50 crore (S.21)
- Penalty schedule: Data Principal violations (false / frivolous / impersonation) — U
- Roles and enforcement: Data Principal — The individual whose personal data is processed (Definitions)
- Roles and enforcement: Data Fiduciary — Decides the purpose and means of processing (Definitions)
- Roles and enforcement: Data Processor — Processes personal data on the Fiduciary's behalf (Definitions)
- Roles and enforcement: Significant Data Fiduciary — Notified by Government on volume/sensitivity; carries extra duties (S.10 / R.13)
- Roles and enforcement: Data Protection Board of India — Independent digital office that adjudicates non-compliance (S.18-S.20)
- Roles and enforcement: Appeals — Telecom Disputes Settlement and Appellate Tribunal (TDSAT), within 60 days (S.22)
- Consent and notice: Consent standard — Free, specific, informed, unconditional, unambiguous, by clear affirmative action (S.6)
- Consent and notice: Withdrawal — As easy as giving consent, at any time (S.6)
- Consent and notice: Notice content — Plain language; itemized data, purposes, rights route, and Board complaint route (S.5 / R.3)
- Consent and notice: Consent Manager — Register with Board; ¹2 crore net worth; i (R.4)
- Children and Significant Data Fiduciaries: Children's threshold — Under 18; verifiable guardian consent required (S.9)
- Children and Significant Data Fiduciaries: Children's prohibitions — No tracking, behavioural monitoring, or targeted advertising (S.9)
- Children and Significant Data Fiduciaries: Guardian verification — Verify guardian identity and age via reliable mechanisms (R.10)

- Children and Significant Data Fiduciaries: SDF duties — India-based DPO, independent annual audit, periodic DPIAs (S.10 / R.13)
- Cross-border transfers and exemptions: Transfer model — Negative list — allowed except to restricted jurisdictions; document each transfer (S.16 / R.15)
- Cross-border transfers and exemptions: Legitimate uses without consent — Voluntary provision, State functions, court orders, medical emergencies, employment (S.7)
- Cross-border transfers and exemptions: Exemptions — National security, research/archival/statistical, notified startups, legal claims, courts, offence investigation (S.17)

Reusable implementation templates

- DPDP Scope And Ownership Memo: Define what is in scope, who owns each workstream, and what evidence must be maintained.
- Purpose And Consent Register: Track purposes, notices, consent status, withdrawal, source systems, and downstream propagation.
- Rights And Grievance Playbook: Operate DSAR, correction, erasure, withdrawal, grievance, and nomination requests.
- DPDP Breach Runbook: Run breach triage, containment, notification decisioning, communication, and remediation.
- Processor And Subprocessor Register: Track third parties handling personal data and their risk, agreements, regions, and offboarding evidence.
- Board-Ready DPDP Status Report: Summarize readiness, critical gaps, owners, due dates, evidence status, and next decisions.

Application walkthrough

Open the organisation workspace to create notices and purpose-specific consent forms, review employee and subscriber audiences separately, test QR/web/mobile/SMS/IVRS journeys, run read-only discovery, prepare DPIA/ROPA evidence and review the launch acceptance register.

The handbook does not include customer records, source-system samples, credentials or provider configuration.