INTERNAL TEAM WORKSHEET

DPDP Rules 2025 Implementation Checklist

What Legal, Product, Engineering, Security, Marketing, Support, HR, And Leadership Need To Build

USE THIS FOR

Cross-functional teams converting the DPDP Rules 2025 into implementation work.

Give businesses a function-by-function checklist for implementing the DPDP Rules before the main full-compliance deadline.

RECOMMENDED WORKFLOW

Complete the worksheet, assign owners, and preserve evidence.

This asset is designed to be shared with internal legal, product, operations, security, and leadership teams.

Important note: Use with current law, official rules, and qualified review for high-risk decisions.

Page 1: Leadership And Governance

TASK	OWNER	STATUS	EVIDENCE
Assign DPDP programme owner			
Create cross-functional DPDP working group			
Approve implementation budget			
Define risk acceptance process			
Create leadership reporting cadence			
Identify whether SDF readiness review is needed			
Approve breach escalation route			
Approve data retention and deletion principles			

Page 2: Legal And Privacy

TASK	OWNER	STATUS	EVIDENCE
Map personal data categories			
Map processing purposes			
Identify legal basis for each purpose			
Separate consent-based processing from Section 7 legitimate uses			
Draft standalone DPDP notice			
Create notice versioning process			
Create consent wording by purpose			
Create withdrawal language			
Define rights request policy			
Define grievance redressal process			
Define retention exceptions			
Review processor contract clauses			
Prepare breach notification templates			
Prepare Board-response evidence process			

Page 3: Product

TASK	OWNER	STATUS	EVIDENCE
Show DPDP notice at the right collection points			
Separate consent purposes in UI			
Avoid pre-ticked consent boxes			
Build consent withdrawal flow			
Add privacy settings or consent management surface			
Create rights request intake path			
Create grievance intake path			
Design nominee capture/update flow if applicable			
Identify child-user journeys			
Add age/parental-consent checks where required			
Confirm marketing consent is separate from service communication			
Make privacy choices accessible from account settings			

Page 4: Engineering And Data

TASK	OWNER	STATUS	EVIDENCE
Create system inventory for personal data			
Create consent event log			
Store notice version shown at consent			
Connect withdrawal to downstream systems			
Build user data lookup for access requests			
Build correction/update workflow			
Build erasure/anonymisation jobs			
Map data warehouse copies			
Map analytics identifiers			
Define backup handling for erasure requests			
Create audit logs for rights actions			
Create affected-user extraction process for breaches			
Add processor deletion/export API notes			

Page 5: Security And Incident Response

TASK	OWNER	STATUS	EVIDENCE
Review access controls for personal data systems			
Review encryption and key-management controls			
Review logging and monitoring			
Define personal data breach criteria			
Create incident triage workflow			
Create 72-hour Board notification workflow			
Create affected Data Principal notification workflow			
Add vendor breach notification SLAs			
Run breach tabletop exercise			
Preserve breach decision evidence			

Page 6: Support And Operations

TASK	OWNER	STATUS	EVIDENCE
Train support team on Data Principal requests			
Create request triage categories			
Create identity verification playbook			
Create access response template			
Create correction response template			
Create erasure response template			
Create grievance response template			
Create escalation path to privacy/legal			
Create request tracker			
Test a mock rights request			

Page 7: Marketing And Sales

TASK	OWNER	STATUS	EVIDENCE
Separate marketing consent from service communications			
Review lead forms and demo request forms			
Map ad audiences and retargeting data			
Map newsletter and campaign tools			
Create suppression and withdrawal process			
Review enrichment tools and list sources			
Review partner-sharing practices			
Update sales handoff data rules			
Remove stale leads under retention policy			

Page 8: HR And Employee Data

TASK	OWNER	STATUS	EVIDENCE
Map employee personal data			
Identify employment-purpose processing under Section 7			
Review payroll and benefits processors			
Create employee access/correction process			
Define employee retention schedule			
Review monitoring and access-control policies			
Review background verification process			
Create employee grievance route for data issues			

Page 9: Vendor And Processor Management

TASK	OWNER	STATUS	EVIDENCE
Create vendor inventory			
Identify processors holding personal data			
Map data categories shared with each vendor			
Add DPDP processor clauses			
Add breach notification SLA			
Add rights request assistance clause			
Add deletion/return clause			
Add subprocessor disclosure requirement			
Add audit evidence requirement			
Test vendor deletion confirmation			

Page 10: Milestone Plan

PERIOD	MILESTONE
Months 1-2	Data map, system inventory, vendor inventory, risk classification
Months 3-4	Notice rewrite, consent flow, withdrawal flow, purpose mapping
Months 5-6	Rights request intake, grievance mechanism, support templates, vendor SLAs
Months 7-8	Retention schedule, deletion/anonymisation jobs, backup treatment
Months 9-10	Breach workflow, 72-hour templates, security evidence, tabletop test
Months 11-12	Mock audit, mock rights request, mock erasure, remediation report

Footer Disclaimer

This checklist is for implementation planning only. Adapt it to your systems, contracts, sectoral obligations, and legal advice before use.