

INTERNAL TEAM WORKSHEET

# DPDP Act 2023 Section Map And Compliance Timeline

The Business Guide To Sections, Owners, Evidence, And Deadlines

## USE THIS FOR

**Founders, legal, product, and engineering teams aligning on DPDP scope and owners.**

Help founders, legal teams, product teams, and operators understand which DPDP Act sections drive which implementation work.

## 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: Core Section Map

DPDP SECTION	TOPIC	BUSINESS MEANING	PRIMARY OWNER	EVIDENCE TO MAINTAIN
Section 3	Applicability	Determine whether digital personal data processing is in scope	Legal/privacy	Scope memo, processing inventory
Section 4	Grounds for processing	Process personal data only with consent or legitimate use	Legal/product	Legal basis map
Section 5	Notice	Give clear notice before or with consent	Legal/product	Notice versions, screenshots, publishing logs
Section 6	Consent	Collect valid, specific, informed, clear consent	Product/engineering	Consent logs, notice version, withdrawal records
Section 7	Legitimate uses	Use specific consent exceptions only where they fit	Legal/privacy	Section 7 decision records
Section 8	General obligations	Security, breach, processor, erasure, grievance, compliance duties	Leadership/security/privacy	Controls, breach plan, processor contracts, erasure logs
Section 9	Children's data	Extra protection for users under 18	Product/legal	Age handling, parental consent records, ad/profiling controls
Section 10	Significant Data Fiduciaries	Extra governance if notified as SDF	Leadership/privacy	DPO model, auditor plan, DPIA, audit evidence
Section 11	Access right	Data Principal can seek information about personal data	Support/privacy	Access request logs and responses
Section 12	Correction and erasure	Correct, complete, update, and erase data where required	Support/engineering	Correction and erasure records
Section 13	Grievance redressal	Provide readily available grievance mechanism	Support/privacy	Grievance logs, escalation records
Section 14	Nomination	Allow nomination for death/incapacity scenarios	Product/support	Nominee records, verification process
Section 15	Duties of Data Principals	Individuals must not impersonate or file false complaints	Support/legal	Fraud/abuse notes, refusal records
Section 16	Cross-border transfer	Watch for notified country/territory restrictions	Legal/vendor management	Transfer map, vendor locations
Section 17	Exemptions	Some processing may be exempt in specific cases	Legal	Exemption memo where relied upon
Sections 18-32	Data Protection Board	Board structure, powers, process, appeals, voluntary undertakings	Legal/leadership	Board correspondence, undertaking records
Section 33 + Schedule	Penalties	Monetary penalties for non-compliance categories	Leadership/legal	Risk register, remediation evidence

## Page 2: Compliance Timeline

PHASE	DATE	WHAT BUSINESSES SHOULD DO
Foundation	Now	Build personal data inventory, vendor inventory, and legal basis map
DPDP Rules foundation	November 2025	Track Board framework, governance, and implementation planning
Consent Manager phase	November 2026	Prepare if operating in consent infrastructure; clean consent records if acting as Data Fiduciary
Main compliance phase	May 2027	Have notice, consent, withdrawal, rights, erasure, breach, grievance, security, and vendor controls operational
Post-enforcement	Ongoing	Maintain evidence, audits, rights logs, vendor confirmations, incident records, and notice updates

## Page 3: Implementation Owners

OWNER	DPDP RESPONSIBILITIES
Leadership	Budget, risk acceptance, programme owner, SDF readiness, escalation
Legal/privacy	Scope, notices, consent language, Section 7 decisions, contracts, Board response
Product	Consent UI, notice placement, privacy settings, rights intake, children's data journeys
Engineering/data	Consent logs, data map, deletion jobs, access exports, audit logs, data warehouse controls
Security	Safeguards, access controls, incident response, breach evidence, monitoring
Support/operations	Rights request intake, verification, response templates, grievance handling
Marketing/sales	Consent for outreach, lead-source records, suppression, ad audience controls
HR	Employee data, payroll/benefits processors, employee rights, internal grievance handling
Vendor management	Processor contracts, deletion support, breach SLAs, audit evidence

## Page 4: Penalty Snapshot

CATEGORY	MAXIMUM PENALTY	WHAT TO PREVENT
Security safeguard failure causing personal data breach	Up to Rs. 250 crore	Weak access controls, missing security safeguards, unmanaged vendor risk
Failure to notify breach	Up to Rs. 200 crore	No 72-hour workflow, no affected-user identification, delayed vendor notice
Children's data obligation breach	Up to Rs. 200 crore	No parental consent, targeted ads to children, harmful processing
SDF obligation breach	Up to Rs. 150 crore	No DPO, no independent auditor, no DPIA/audit readiness
Other DPDP provision or undertaking breach	Up to Rs. 50 crore	Broken notices, consent, rights, erasure, grievance, or undertaking commitments
Data Principal duty breach	Up to Rs. 10,000	False complaints, impersonation, false information by individual

## Page 5: First 30 Days Checklist

---

DAY RANGE	ACTION	OUTPUT
Days 1-5	Assign DPDP programme owner	Named owner and leadership sponsor
Days 1-10	Map personal data categories	Data category inventory
Days 5-15	Map systems and vendors	System and processor inventory
Days 10-20	Map purposes and legal bases	Consent/Section 7 basis map
Days 15-25	Review notices and consent flows	Notice and UI gap list
Days 20-30	Identify top 10 remediation items	Implementation backlog

## Page 6: Evidence Pack Checklist

---

EVIDENCE ITEM	READY?	LOCATION
Personal data inventory	Yes / No	
Processing purpose map	Yes / No	
Consent records	Yes / No	
Notice versions	Yes / No	
Section 7 decision records	Yes / No	
Rights request tracker	Yes / No	
Grievance logs	Yes / No	
Retention schedule	Yes / No	
Erasure logs	Yes / No	
Processor/vendor contracts	Yes / No	
Breach response plan	Yes / No	
Breach notification templates	Yes / No	
Children's data assessment	Yes / No	
SDF readiness assessment	Yes / No	
Security control evidence	Yes / No	

## Footer Disclaimer

---

This section map is for general DPDP implementation planning. It should be reviewed against official law, current rules, sectoral regulations, and qualified legal advice before use.