Technology & Digital Platforms

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For IT companies, SaaS providers, app developers, e-commerce, AI firms, payment gateways, and digital platforms.

1. Overview & Applicability

Technology and digital platform companies are at the very core of DPDPA applicability. Whether you operate a SaaS product, a mobile application, an e-commerce marketplace, or an AI service, you collect, process, and store vast quantities of personal data. The DPDPA classifies you as a 'Data Fiduciary' and requires strict compliance. Large platforms are likely to be designated as Significant Data Fiduciaries (SDFs) with additional obligations.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

Data Fiduciary	Any entity determining the purpose and means of processing personal data — this includes you.
Data Principal	The individual whose data you collect — your users, customers, or subscribers.
Personal Data	Any data that can identify an individual — names, emails, IDs, device IDs, IP addresses, usage logs.
Consent	Freely given, specific, informed, and unambiguous agreement — a pre-ticked box is NOT valid consent.
Data Processor	A third party (e.g., AWS, analytics vendor) processing data on your behalf.
Significant Data Fiduciary (SDF)	Designated by the Central Government based on volume, sensitivity, and risk of data processed.
Purpose Limitation	Data can only be used for the purpose stated at the time of collection.

3. Core Compliance Obligations

Every entity in this sector that processes personal data must comply with the following obligations:

1. **Consent Management System**
   Implement a granular, purpose-specific consent mechanism. Maintain time-stamped consent records. Ensure users can withdraw consent easily. Bundled consent is prohibited.
2. **Privacy Notice**
   Publish a clear, plain-language privacy notice disclosing: data categories collected, purpose, rights of users, grievance officer contact, and data processor details.
3. **Data Minimisation**
   Collect only the minimum data needed. Conduct regular data audits to remove unnecessary fields.
4. **Security Safeguards**
   Implement encryption (at rest and in transit), access controls, vulnerability assessments, and incident response plans.
5. **Breach Notification**
   Report personal data breaches to the DPBI and affected users without unreasonable delay. Maintain a breach register.
6. **Data Principal Rights**
   Build mechanisms for users to request: access, correction, erasure, grievance redressal, and nomination. Respond promptly.

7	**Data Processor Contracts** Execute written Data Processing Agreements (DPAs) with all third-party processors (cloud providers, analytics, marketing tools).
8	**Children's Data** If your platform is accessible to children (under 18), obtain verifiable parental consent. No behavioural tracking of children.
9	**Cross-Border Transfers** Ensure data is only transferred to countries approved by the Central Government. Add contractual safeguards.
10	**SDF Obligations (if designated)** Appoint an India-based DPO, conduct periodic Data Audits, perform DPIAs, and ensure algorithmic transparency.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Audit all personal data flows — map what data you collect, where it is stored, who processes it, and for how long.
- ☐ Update your Privacy Policy / Notice to comply with DPDPA requirements — plain language, complete, accessible.
- ☐ Implement granular consent banners / flows — separate consent for each purpose, easy withdrawal option.
- ☐ Appoint a Grievance Officer and publish contact details on your website and app.
- ☐ Sign Data Processing Agreements with all third-party vendors handling personal data.
- ☐ Enable Data Principal Rights: access portal, correction request, erasure / account deletion flows.
- ☐ Implement personal data breach detection, response, and notification procedures.
- ☐ Conduct a children's data audit — verify if your platform serves under-18 users and implement parental consent.
- ☐ Review cross-border data transfers — confirm all destination countries are on the approved list.
- ☐ Conduct a DPIA for all high-risk processing activities (AI/ML profiling, behavioural targeting, biometrics).
- ☐ If likely SDF: appoint an India-resident DPO and prepare for periodic independent audits.
- ☐ Train all engineering, product, and customer support teams on DPDPA obligations.

5. Applicable Penalties

The Data Protection Board of India (DPBI) may impose the following penalties for non-compliance:

Rs. 250 Crore	Failure to implement reasonable security safeguards resulting in a personal data breach
Rs. 200 Crore	Breach of obligations related to processing children's personal data
Rs. 150 Crore	Failure to fulfill obligations as a Significant Data Fiduciary (SDF)
Rs. 50 Crore	Failure to comply with Data Principal rights or other provisions of the Act

6. Implementation Roadmap

Follow this phased approach to achieve full DPDPA compliance:

1	**Month 1–2: Data Mapping** Conduct a complete data inventory — identify all personal data, processing activities, third parties, and retention periods.
2	**Month 2–3: Gap Analysis** Compare current practices against DPDPA requirements. Identify compliance gaps in consent, notice, security, and rights.
3	**Month 3–4: Policy & Process Overhaul** Update privacy notice, consent flows, retention policies, and internal data handling procedures.
4	**Month 4–5: Technical Implementation** Build consent management, rights request portals, breach detection systems, and DPA workflows.

5	**Month 5–6: Training & Testing** Train staff. Conduct penetration testing, consent audit, and a mock breach drill.
6	**Month 6+: Ongoing Compliance** Quarterly reviews, annual audits, Board/SDF obligations monitoring, and stay updated on Rules as notified.

💡 Pro Tip: Document everything. Under the DPDPA, the burden of proof that consent was obtained lies with the Data Fiduciary. A well-maintained consent log is your strongest protection.