Banking, Finance & Insurance (BFSI)

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For banks, NBFCs, insurers, stock brokers, mutual funds, credit bureaus, and lending platforms.

1. Overview & Applicability

The BFSI sector processes some of the most sensitive personal and financial data — KYC documents, transaction records, credit histories, and insurance claims. DPDPA operates alongside existing sectoral regulators (RBI, SEBI, IRDAI, PFRDA). Where sectoral law and DPDPA overlap, the more protective standard applies. Entities such as credit bureaus and large banks are likely SDF candidates.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

Financial Personal Data	Account numbers, transaction records, credit scores, loan history, insurance policy details — all constitute personal data.
KYC Data	Aadhaar, PAN, passport details collected for know-your-customer — subject to strict purpose limitation.
Sensitive Financial Data	Bank account details, credit/debit card data, and financial history require enhanced protection.
Purpose Limitation	Data collected for loan processing cannot be used for marketing without fresh consent.
Data Processor	Credit bureaus, payment processors, outsourced KYC vendors — all require written DPAs.
Legitimate Use	Certain processing (e.g., fraud prevention, regulatory compliance) may be lawful without consent under prescribed grounds.

3. Core Compliance Obligations

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

1. **KYC Data Governance**
   KYC data must be stored only for the period required by RBI/SEBI guidelines. After that, delete or anonymise. Restrict access to authorised personnel only.
2. **Marketing Consent**
   Consent must be obtained separately for marketing communications. Pre-ticked opt-in for promotional offers is invalid.
3. **Credit Data Accuracy**
   Ensure data shared with credit bureaus is accurate. Implement a process to correct erroneous credit information upon Data Principal request.
4. **Insurance Claims Data**
   Process claims data strictly for claims management. Do not share health data with marketing teams without explicit consent.
5. **Fraud Detection**
   Automated fraud detection using personal data may be a legitimate use — but must be documented and disclosed.
6. **Data Sharing with Regulators**
   Sharing data with RBI/SEBI/IRDAI for regulatory compliance is a lawful basis. Document each instance.
7. **Third-Party Fintech Integration**
   Execute DPAs with all fintech partners, payment aggregators, and analytics providers.

8	**Breach Response** Financial data breaches must be reported to DPBI. Coordinate with RBI/SEBI breach reporting requirements simultaneously.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Audit all KYC data stores — verify retention periods comply with RBI guidelines AND DPDPA storage limitation.
- ☐ Separate marketing consent from transactional consent in all onboarding flows.
- ☐ Review all DPAs with credit bureaus, payment processors, and outsourced KYC vendors.
- ☐ Publish a DPDPA-compliant privacy notice on your website, app, and branch materials.
- ☐ Appoint a Grievance Officer — ensure contact details are displayed prominently.
- ☐ Build a process for customers to request correction of financial data (especially credit records).
- ☐ Implement access controls — only authorised staff can access customer financial data.
- ☐ Conduct annual security audits and penetration tests of core banking systems.
- ☐ Review cross-border data sharing arrangements with correspondent banks and reinsurers.
- ☐ Align DPDPA compliance with RBI/SEBI/IRDAI data protection circulars.
- ☐ Train relationship managers and customer service teams on data rights and grievance handling.

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: Regulatory Mapping** Map DPDPA obligations against existing RBI, SEBI, IRDAI directives to identify overlaps and gaps.
2	**Month 2: Data Inventory** Catalogue all personal and financial data — KYC, transaction, insurance, and credit data flows.
3	**Month 3: Consent & Notice Overhaul** Redesign onboarding consent flows and update all privacy notices across web, app, and branch.
4	**Month 4: Vendor & DPA Review** Audit all third-party data processors and execute or update Data Processing Agreements.
5	**Month 5: Technical Controls** Implement access controls, encryption standards, and breach notification workflows.
6	**Month 6+: Audit & Monitor** Quarterly compliance reviews aligned with regulatory examination cycles.

⚠️ Note: DPDPA compliance does not replace RBI / SEBI / IRDAI obligations. Run a parallel compliance programme and document where requirements overlap or differ.

Disclaimer: *This handbook is for awareness and informational purposes only. It does not constitute legal advice. Please consult a qualified data protection lawyer for specific compliance guidance. | DPDPA 2023 · India*