KGS CONSULTING

# Digital Personal Data Protection (DPDP) ACT, 2023

BFSI SECTOR COMPLIANCE GUIDE
JUNE 2026


consultkgc.com

# Table of Contents


1. Executive Summary 01

2. DPDPA Provisions Mapped to BFSI Operations 02

3. Segment-Wise Applicability & Use Cases 04

- Banking
- Insurance
- NBFC (Non-Banking Financial Company)
- FinTech (Neobank / Digital Lender)
- Wealth Management
- Capital Markets (Stock Exchanges, Depositories, Clearing Corps)
- Lending (P2P, BNPL, Microfinance, Gold Loan)
- Payments (Gateways, Processors, PPI Issuers, Acquirers)
- Insurtech
- Credit Rating Agencies (CICs – CIBIL, Experian, CRIF, Equifax)

4. Compliance Gap Assessment Checklist 10

5. Technology Enablers for DPDP Compliance 12

6. Conclusion – The Path to Readiness 14

# 1. Executive Summary

India is at a pivotal moment in its digital governance journey. The Digital Personal Data Protection (DPDP) Act, 2023, notified on 11 August 2023, is India's first comprehensive privacy law. After the rule-making process, MEITY announced the Digital Personal Data Protection Rules, 2025, on November 13, 2025, creating the compliance framework. The DPDP Act works within a layered regulatory landscape, including RBI, SEBI, IRDAI, and CERT-In, requiring coordinated compliance.

While enforcement is expected in 2027, entities that delay requisite preparation risk regulatory, financial, and reputational consequences when enforcement begins. Those viewing DPDP as an add-on will struggle more than those adopting it as a governance transformation with board support, cross-functional ownership, and technology enablement.

For the BFSI sector, the DPDP Act isn't just compliance; it's a fundamental shift in handling personal data. BFSI firms process vast amounts of sensitive personal data (Aadhaar, PAN, financials, credit scores, biometrics, etc.). Under DPDP, every bank, insurer, NBFC, FinTech, and credit bureau is a Data Fiduciary, who is accountable for consent, purpose limitation, data retention, breach notification, and upholding data principal rights. This guide is structured to assist BFSI leadership in understanding the Act's implications across their specific business segments, assessing their current readiness gaps, and deploying the right technology and governance interventions before enforcement begins.

**The window for structured, cost-effective preparation is now.**

## KEY HIGHLIGHTS

- DPDP Act, 2023, notified August 2023; DPDP Rules, 2025, notified November 2025; full enforcement expected in 2027
- All BFSI entities - banks, insurers, NBFCs, FinTechs, payment processors, credit bureaus - are Data Fiduciaries
- Penalties up to INR 250 crore per violation for non-compliance
- 72-hour breach notification obligation to the Data Protection Board and affected data principals
- Compliance is multi-layered: DPDP must be coordinated with RBI, SEBI, IRDAI, and CERT-In frameworks
- A structured readiness programme is the most effective approach

# 2. DPDPA Provisions Mapped To BFSI Operations

Understanding the DPDP Act's architecture is essential for compliance. It enforces a consent-first data regime, asserting that personal data belongs to individuals and can be processed only with explicit consent or in legal cases. The Act creates a clear accountability structure: a Data Fiduciary, responsible for data processing, and Data Processors, who handle data on fiduciaries' behalf under written agreements. When a BFSI entity acts as both fiduciary and processor (as in co-lending and account aggregator setups), it must fulfil dual obligations.

The table below links the Act's main points to BFSI.

| DPDP Provision | BFSI Application | Example |
|---|---|---|
| Consent (Sec 4-6) | Must be free, specific, informed, unconditional, and revocable | Separate consent for account opening, credit card, and loan offers |
| Notice (Sec 5) | Clear notice at data collection with purpose, retention, rights | KYC form includes DPDP notice with QR code for full policy |
| Data Principal Rights (Sec 12-15) | Right to access, correct, erase, port, and grievance | Customer can request deletion of transaction history after account closure |
| Retention & Deletion (Sec 8) | Delete data as soon as purpose ends, unless required by law | Delete loan application dataafter 3 years (RBI says 3 years for rejected loans) |
| Breach Reporting (Sec 8(6) | Notify Board and affected individuals within 72 hours | Unauthorized access to core banking system triggers breach report |
| Data Localization (Sec 16) | All personal data stored in India (no cross-border transfer except whitelisted countries) | Payment data cannot be replicated to foreign cloud region |
| Processing Agreements (Sec 8) | Written contract with every data processor | Agreement with cloud vendor, TPA, analytics provide |
| Significant Data Fiduciary (Sec 9-10) | Additional obligations: DPIA, data audit, privacy by design, consent manager | Large bank with >10M customers appoints independent data auditor |

# 3. Segment-Wise Applicability & Use Cases

The BFSI sector is diverse, comprising a broad range of entities - from large public sector banks and life insurers serving hundreds of millions of customers to nimble FinTech startups, specialised NBFCs, and market infrastructure entities such as stock exchanges and credit bureaus. Although the DPDP Act applies equally to all Data Fiduciaries, the practical compliance requirements differ considerably among these sub-segments due to variations in data types, operational workflows, and relevant regulations. This segment-by-segment analysis links the Act's obligations to specific operational scenarios across ten BFSI sub-sectors, helping leadership teams understand their compliance duties within their respective business context.


## 1. Banking

**Use Case:** Savings account opening via mobile app

**Data Processed:** Name, Aadhaar, PAN, photo, signature, mobile, email, income proof

**DPDP Compliance Rules:**
• Explicit consent for each purpose (account operations, credit card offers, third-party products)
• Notice in English & local language – must specify data sharing with credit bureaus
• Enable online consent withdrawal & account closure data deletion (after legal retention)
• Breach reporting to RBI & affected customers within 72 hours

## 2. Insurance

**Use Case:** Health insurance claim processing

**Data Processed:** Medical history, family details, hospitalization records, nominee info, employer details

**DPDP Compliance Rules:**
• Sensitive data (health) – explicit, separate consent for TPA/hospital sharing
• Purpose limitation – medical data cannot be used for marketing or underwriting other products
• Data processing agreements with all third parties (TPAs, re-insurers, investigators)
• Right to correction – customer can fix wrong medical records in claim history

## 3. NBFC (Non-Banking Financial Company)

**Use Case:** Personal loan disbursement- digital guideline

**Data Processed:** Credit bureau report, 6-month bank statements, salary slips, employer contacts, guarantor details

**DPDP Compliance Rules:**
• Separate consent for “credit check with bureau” vs “loan sanction”
• Inform customer about data retention period (as per NBFC master direction)
• Right to erasure after loan closure + 3 years (unless default or legal hold)
• Automated decision disclosure, if AI/ML is used for underwriting.

## 4. FinTech (Neobank / Digital Lender)

**Use Case:** Account aggregator-based loan approval

**Data Processed:** Transaction-level data from other banks, UPI IDs, card tokens, SIP details

**DPDP Compliance Rules:**

- Mandatory Consent Manager integration for AA flows (as per RBI and DPDP)
- No purpose creep; cannot use transaction data for cross-selling without fresh consent
- Data localization; all financial PII stored in India
- Privacy by design; required for significant data fiduciaries (Fintechs with >10M users)

## 5. Wealth Management

**Use Case:** Portfolio advisory service

**Data Processed:** Risk profile, investment goals, net worth, Demat details, PAN, FATCA declaration

**DPDP Compliance Rules:**
- Net worth & investments is sensitive data, therefore explicit consent is required
- Granular consent – separate for advisory, execution, and cross-selling (mutual funds, PMS)
- Data portability – customer can download portfolio history and transfer to another advisor
- Annual privacy audit (mandatory for SEBI-registered RIAs with >500 clients)

## 6. Capital Markets (Stock Exchanges, Depositories, Clearing Corps)

**Use Case:** Investor trading & settlement

**Data Processed:** Demat holdings, buy/sell orders, margin details, UCC, biometric of authorized persons

**DPDP Compliance Rules:**
• Notice must explain data sharing with exchanges, clearing corporations, and SEBI
• Retention as per SEBI (8 years for trade records) – DPDP allows longer if required by law
• Breach reporting to SEBI, CERT-In, and affected investors in parallel
• Purpose-based access – trade data cannot be used for marketing without consent

## 7. Lending (P2P, BNPL, Microfinance, Gold Loan)

**Use Case:** BNPL at checkout (e-commerce)

**Data Processed:** Mobile number, device ID, location, purchase amount, repayment history, default flags

**DPDP Compliance Rules:**
• Consent for credit decision must be informed. Eg: “your data will be checked with credit bureau”
• Deletion of data after loan closure + max 3 years (unless default or legal hold)
• No sharing of repayment data with third-party marketers
• Grievance redressal: appoint Nodal Officer (displayed on app/website)

# 8. Payments (Gateways, Processors, PPI Issuers, Acquirers)

**Use Case:** Payment gateway transaction processing

**Data Processed:** Card number (tokenized), UPI ID, customer name, email, IP address, transaction amount, merchant name

**DPDP Compliance Rules:**
• Tokenization enforced for card storage – DPDP reinforces "de-identification" standard
• Zero retention of CVV or PIN (already RBI prohibited; DPDP adds penalty layer)
• Recurring payments consent must be explicit, revocable, and logged
• Data localization: payment data cannot leave India (including backups)

# 9. Insurtech

**Use Case:** Usage-based motor insurance (telematics)

**Data Processed:** GPS location, driving speed, braking patterns, trip history, phone sensors (accelerometer)

**DPDP Compliance Rules:**
• Location & driving behavior is sensitive data, therefore explicit consent required
• Granular consent – separate for "premium calculation" vs "roadside assistance" vs "driving tips"
• Customers can request deletion of telematics data after policy ends
• Privacy policy must explain use of AI/algorithm in premium determination

KGS CONSULTING

## 10. Credit Rating Agencies (CICs – CIBIL, Experian, CRIF, Equifax)

**Use Case:** Credit score calculation & reporting

**Data Processed:** Loan accounts, credit card limits, repayment history, inquiries, PAN, name, address, DOB

**DPDP Compliance Rules:**

• Consent required before accessing bureau data (already exists, but DPDP mandates explicit, logged consent)
• Right to correction: individuals can dispute and correct errors in credit report (with supporting documents)
• Retention: negative data can be retained only for period specified by RBI (typically 7 years)
• Data principal rights – individual can request a report of who accessed their credit file in last 12 months
• Breach notification – any unauthorized access to bureau database must be reported to affected individuals and
the Data Protection Board

These ten segments collectively demonstrate DPDP's extensive influence within the BFSI ecosystem. Each sub-sector encounters unique issues such as consent management, data retention, and breach notifications, though their operational implementations vary significantly. For example, a payment processor focuses on tokenisation and localisation; an insurer emphasises purpose limitation and TPA governance; a credit bureau prioritises the right-to-correction process and access logging. To be effective, compliance programmes must be tailored to each segment rather than being generic, ensuring they are sustainable in practice.

# 4. Compliance Gap Assessment Checklist

Before deploying technology or redesigning governance, BFSI entities must establish a compliance baseline. The gap assessment is core to DPDP readiness: it compares practices against the Act, highlights remediation needs, and supports board and regulatory reporting. The checklist is an internal self-assessment tool for all BFSI sub-segments. Compliance and audit teams should involve business, legal, IT, and risk functions, as answers rarely lie in one department.

| Area | Requirement | Current Status (Yes/No/Partial) | Next Action Steps |
|---|---|---|---|
| Data Inventory | Complete RoPA (Record of Processing Activities) | | |
| Consent | Consent captured for each Consent purpose, with timestamp and version | | |
| Notice | Privacy notice meets DPDP standards (language, purpose, retention, rights) | | |
| Withdrawal | Mechanism for customers to withdraw consent easily | | |
| Access | Process to provide data principal copy of their data | | |
| Correction | Process to correct inaccurate personal data | | |
| Erasure | Process to correct inaccurate personal data | | |

| Area | Requirement | Current Status (Yes/No/Partial) | Next Action Steps |
|---|---|---|---|
| Portability | Ability to export data in common format | | |
| Grievance | Appointed Grievance Officer, contact details published | | |
| Breach Response | 72-hour internal breach detection & reporting process | | |
| Third-party contracts | All processor contracts have DPDP clauses | | |
| Data localization | All personal data stored only in India | | |
| Retention policy | Policy aligned with RBI/SEBI/IRDAI + DPDP deletion timeline | | |
| Security Controls | Encryption, access logs, DLP, purpose-based controls | | |
| Employee Training | Employee and management awareness program | | |
| Audit Mechanism | Annual DPDP audit mechanism (internal or external) | | |

BFSI entities should treat this checklist as a living document, updated at least annually and following any material change in data processing activities, regulatory guidance, or significant incidents.

# 5. Technology Enablers For DPDP Compliance

DPDP compliance is a governance transformation where technology enables sustainable compliance. For BFSI entities processing data across banking systems, CRM, cloud, third-party, and digital channels, manual compliance is unscalable. A structured tech stack aligned with the Act ensures consistent, evidence-based compliance to regulators, auditors, and customers. The five pillars should be prioritised based on a gap assessment

| Technology Component | Purpose | BFSI-Specific Requirements |
|---|---|---|
| Consent Management Platform (CMP) | Capture, store, version, and operationalise consent withdrawals across all systems | Integration with core banking, CRM, loan origination, and payment systems; granular consent per product; full audit trail for regulatory inspection |
| Data Discovery & Classification | Automatically identify and label personal data across databases, file shares, email systems, and cloud environments | Detect Aadhaar, PAN, card numbers, IFSC, and account numbers; map data flows between systems (e.g., CRM to TPA or credit bureau) |
| DLP & Encryption | Prevent unauthorised sharing and ensure data is protected at rest and in transit | Block unencrypted transmission of Aadhaar or PAN; enforce HTTPS/TLS for all customer-facing applications |
| Purpose-Based Access Control (PBAC) | Restrict employee access to personal data based on the specific business purpose | Loan officer accesses only loan-related data; access to investments or insurance data requires separate authorisation; every access is logged |
| Audit Logging & SIEM | Centralised logging of all access, modification, and deletion of personal data | Log retention for a minimum of three years (or as per applicable regulator); SIEM alerts configured for anomalous access patterns |

It is essential to recognise that mere procurement of technology does not equate to compliance. Using a Consent Management Platform without updating privacy notices, workflows, and training won't meet the Act's requirements. A data discovery tool that categorises data but isn't linked to deletion or access controls offers limited benefits. BFSI leaders should evaluate if tech tools genuinely change data processing or just generate reports, as the former improves compliance, while the latter adds unnecessary burden without reducing risk.

# 6. Conclusion – The Path to Readiness

## Key Takeaways for BFSI Leadership

The DPDP Act, 2023, and the November 2025 Rules form a critical legal and strategic governance framework. For BFSI institutions, it's an enterprise-wide transformation, not just IT compliance, demanding board sponsorship, cross-functional management, and a rethink of consent, data rights, and accountability in customer processes. Enforcement is expected next year, leaving only a few months for preparation.

**The core imperatives for leadership are clear -**

**1. DPDP is non-negotiable:** Penalties up to ₹250 Cr and reputational damage.

**2. Start now:** A 4-phase roadmap (visibility foundation risk reduction audit) takes 6-9 months to be fully ready.

**3. Technology is an enabler:** Consent management, discovery, DLP, and PBAC are critical.

**4. Governance, not just tools:** Policies, training, breach drills, and independent audits are mandatory.

**5. Regulatory overlap:** DPDP works alongside RBI/SEBI/IRDAI guidelines; early alignment gives competitive advantage.

**Recommended Immediate Actions**

- Appoint a Privacy Officer and Grievance Officer.
- Conduct a high-level data discovery to identify all PII stores.
- Run a gap assessment using the checklist (Assessment sheet is shared above).
- Prioritize critical gaps (consent, breach response, retention).

**Get the Support from the Right Expert at the Right Time**

- Gap assessment and RoPA development
- End-to-end implementation or phase-wise engagement
- Technology solutions (consent management, discovery tools)
- Legal & cyber security integration (DPDP + BFSI regulatory alignment)
- Employee Awareness, Training & audit support

# List of Abbreviations

| Abbreviation | Full Form |
|---|---|
| AA | Account Aggregator |
| BFSI | Banking, Financial Services, and Insurance |
| BNPL | Buy Now Pay Later |
| CERT-In | Indian Computer Emergency Response Team |
| CIC | Credit Information Company |
| CISO | Chief Information Security Officer |
| CMP | Consent Management Platform |
| CRA | Credit Rating Agency (used interchangeably with CIC) |
| DLP | Data Loss Prevention |
| DPBI | Data Protection Board of India |
| DPDP | Digital Personal Data Protection |
| DPIADPO | Data Protection Impact Assessment |
| DPO | Data Protection Officer (or Privacy Officer) |
| FinTech | Financial Technology |
| IDS | Intrusion Detection System |
| InsureTech | Insurance Technology |
| IPS | Intrusion Prevention System |
| IRDAI | Insurance Regulatory and Development Authority of India |

| Abbreviation | Full Form |
|---|---|
| ITGC | Information Technology General Controls |
| KYC | Know Your Customer |
| NBFC | Non-Banking Financial Company |
| PAN | Permanent Account Number |
| PBAC | Purpose-Based Access Control |
| PII | Personally Identifiable Information |
| RBI | Reserve Bank of India |
| RoPA | Record of Processing Activities |
| SEBI | Securities and Exchange Board of India |
| SIEM | Security Information and Event Management |
| SOC | Security Operations Center |
| TPA | Third-Party Administrator |
| UIDAI | Unique Identification Authority of India |
| UPI | Unified Payments Interface |

KGS CONSULTING

## Sources and References


**1. DPDP Act, 2023 (No. 22 of 2023)**
(Gazette of India notification published August 11, 2023 – the full official text of the Act)

**2. DPDP Rules, 2025**
(Notified November 13, 2025 by MEITY – operationalizes the Act with specific compliance requirements)

**3. RBI Digital Lending Directions, 2025 (RBI/2025-26/36)**
Data localization & explicit consent requirements for digital lending

**4. RBI – Payment System Data Localization**
Mandates payment system data stored only in India (6-month compliance window).

**Additional references:**
• MEITY Draft DPDP Rules, 2025 – Published January 3, 2025 for public consultation
• CERT-In Breach Reporting Guidelines – For dual reporting requirements (CERT-In + DPB)
• RBI Master Direction on Outsourcing of IT Services – For vendor/third-party compliance alignment with DPDP
• DSCI (Data Security Council of India) – Privacy governance frameworks and Data Privacy Lead Assessor standards
• Consent Manager Framework (BRDCMS) – Business Requirement Document for Consent Management System under DPDP Act

KGS CONSULTING

## KGS Office

### Mumbai

601, 6th Floor, Earth Vintage
Senapati Bapat Marg
Dadar West, Mumbai 400 028

## Get in touch

Siddhi Dalvi

PHONE
+91 9146639547

EMAIL
siddhi.dalvi@consultkgs.com