ADVOCATES & SOLICITORS

MASTERING DIGITAL PERSONAL DATA PROTECTION:

SECTOR-WISE INSIGHTS FOR NBFCS, FINTECHS, PAYMENT PROVIDERS & HEALTHCARE SYSTEMS

Featuring obligations, operational impacts, compliance checklists, data lifecycle management, and strategic recommendations

Prepared by:

Ak & Partners

2025

About the Founders

Anuroop Omkar
Managing Partner

Anuroop is known for his strategic counsel to foreign investors, financial institutions, and fintech companies in India. With a decade of cross-border advisory experience, he has led mandates across banking regulation, digital lending, and insolvency turnaround. His blend of legal insight and commercial foresight makes him a trusted advisor. Anuroop is also a noted speaker and author on fintech policy and RBI regulations. He is committed to delivering fast, viable, and regulatorily sound solutions.

Kritika Krishnamurthy
Managing Partner

Kritika specialises in business advisory, from developing the most efficient strategy to expanding the business with growth capital, along with managing all material risks that come in the way. She advises banks, fintechs, and global investors on regulatory strategy, negotiations, enforcement, and cross-border transactions, with expertise in digital lending, PPI, and financial regulation. A published author and speaker on fintech governance, she is known for her fast, solution-driven, and business-aligned approach.

From the Founder's Desk

"Privacy is no longer a compliance formality — it is an organisational instinct, a cultural commitment, and a promise at the heart of every digital interaction."

Anuroop Omkar
Founding Partner

Kritika Krishnamurthy
Founding Partner

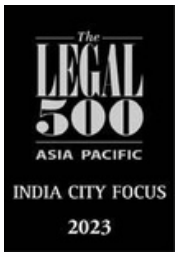
The Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 mark a defining moment in India's regulatory journey. Much like every compounding order tells a deeper story, every clause of this new data protection regime reflects an evolving understanding of how India envisions trust, transparency, and digital accountability.

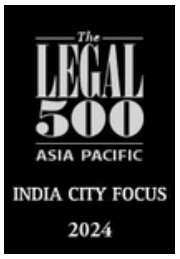
Beyond compliance checklists and implementation calendars lies a more profound narrative: one that challenges organisations to reimagine the very foundations of governance and risk stewardship in a data-driven economy. Each consent notice issued, each security safeguard implemented, and each breach protocol rehearsed becomes a reflection of how seriously an organisation values the dignity and rights of the individuals it serves. Whether an NBFC navigating complex KYC portfolios, a FinTech scaling algorithmic decisioning, a payment provider securing high-velocity transactions, or a healthcare institution safeguarding sensitive medical records—every data touchpoint today carries the weight of expectation. Under DPDP, lapses are no longer mere operational misses; they are signals of deeper gaps in culture, systems, and foresight. We view this regulatory shift not as a constraint but as an opportunity.

The DPDP framework offers organisations a moment for introspection—a chance to rebuild data flows with clarity, redesign consent with honesty, and reinforce systems with resilience. Compliance is no longer a reactive patchwork; it is a forward-looking investment in credibility, risk mitigation, and long-term value creation.

As the roles of Data Fiduciaries, Data Protection Officers, and Consent Managers take shape, the real test will be whether organisations can embed privacy not at the margins, but at the core of decision-making. This report underscores that DPDP compliance is not a finite project, but a continuous journey—one that demands vigilance, empathy, and the courage to evolve.

Awards & Recognitions





Executive Summary

The Digital Personal Data Protection (DPDP) Act, 2023 and the DPDP Rules, 2025 together establish India's most comprehensive framework for governing digital personal data, placing clear and enforceable obligations on all organisations that collect or process such data. The regime mandates purpose-specific, unbundled consent, standalone privacy notices, user-friendly consent withdrawal, and stringent data minimisation practices. It requires businesses to implement reasonable security safeguards—such as encryption, access controls, audit trails, and breach reporting to both users and the Data Protection Board (DPB)—while also granting individuals legally enforceable rights to access, correction, erasure, and grievance redressal.

Sectoral laws such as RBI guidelines, PMLA, and healthcare regulations continue to take precedence where stricter retention or operational requirements apply. Across industries, the implications are significant: NBFCs must harmonise DPDP with RBI's data security and KYC retention mandates while strengthening consent, governance, and breach readiness.

FinTechs face extensive redesign of app flows to ensure unbundled consent, data minimisation, algorithmic accountability, and integration with the emerging Consent Manager ecosystem. Payment systems and PPI issuers must overhaul their onboarding journeys to present standalone notices, enforce strict purpose limitation for transactional data, and enhance incident response and user rights interfaces. Healthcare providers must adopt stronger patient data privacy practices, implement verifiable parental consent for minors, and manage sensitive medical information with digitised, secure, and DPDP-aligned processes while benefiting from emergency-care exemptions.

Across all sectors, the Act and Rules require organisations to invest in data mapping, system upgrades, internal training, processor contract re-engineering, and governance structures—potentially including Data Protection Officers and impact assessments for significant data fiduciaries. While compliance demands substantial operational uplifting, the DPDP framework ultimately enhances consumer trust, reduces legal and reputational risk, and aligns India with global data protection standards, making privacy a central pillar of digital business strategy across NBFC, FinTech, Payments, and Healthcare ecosystems.

Table of Contents

Implementation Calendar

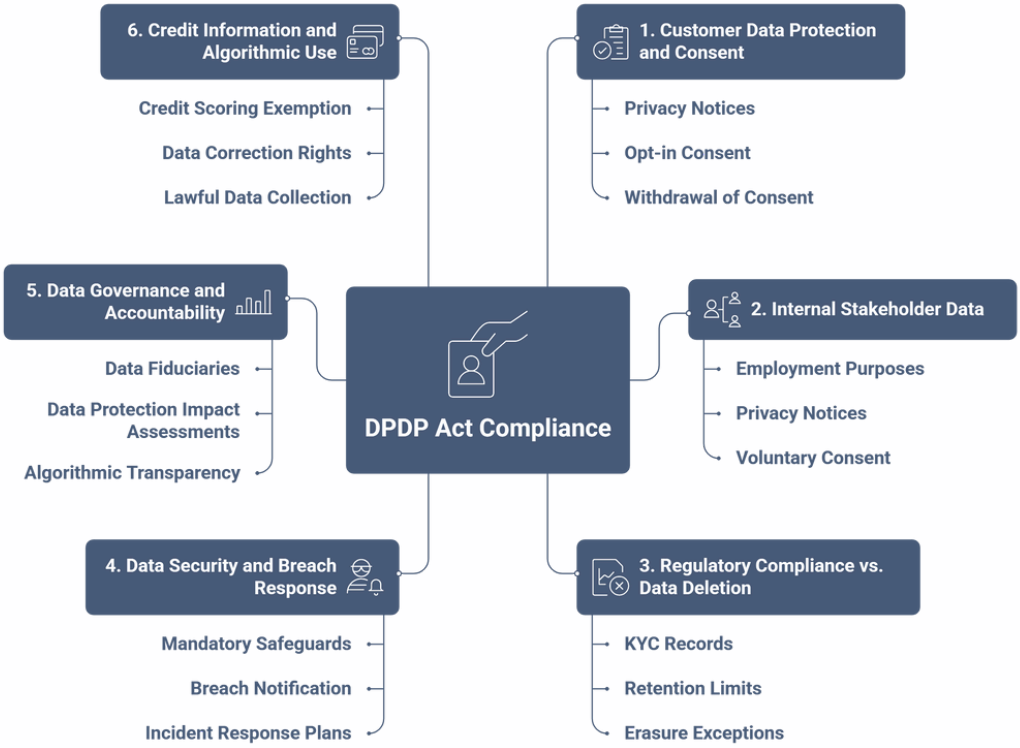
What is in force	From when	Implications for Compliance and Tech
Data Protection Board	Immediately	• Appointment of key officials of the Board to commence. • Expect rollout of advertisements for recruitment of officers. • No compliance at corporate end.
Registration of Consent Managers	November 13, 2026 (12 months from notification)	Fintech having digital infrastructure for consent management to start prepping to get regulatory registration.
Consent Notice while obtaining Personal Data	May 13th, 2027	Commence gap analysis and preparation.
Implementing Reasonable Security Safeguards for Data Fiduciary		
Obligations on Personal Data Breach		
Data purge timelines for notified sectors		
Appointment of Data Protection Officer		
Guidelines on Personal Data Processing of Children and Differently Abled		
Additional Obligations of Significant Data Fiduciary		
Commencement of obligation to supply data for Data Fiduciary and intermediary		

Non-Banking Financial Companies (NBFCs)

A New Strategic Imperative for NBFCs

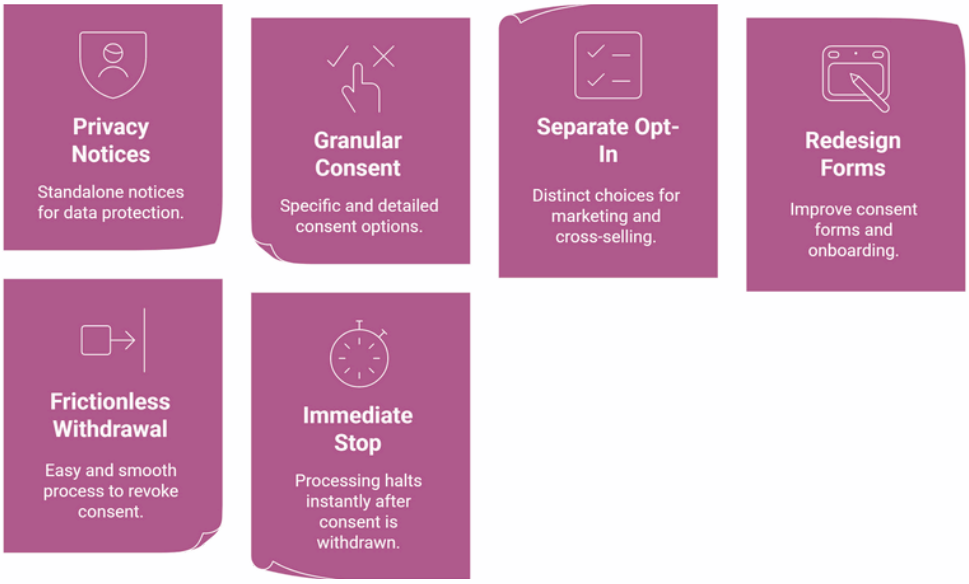
Non-Banking Financial Companies (NBFCs)

NBFCs handle large volumes of sensitive personal and financial data, from customer loan files and KYC documents to employee records. The DPDP Rules, 2025 introduce new regulatory and governance requirements that NBFCs must integrate alongside existing RBI guidelines:



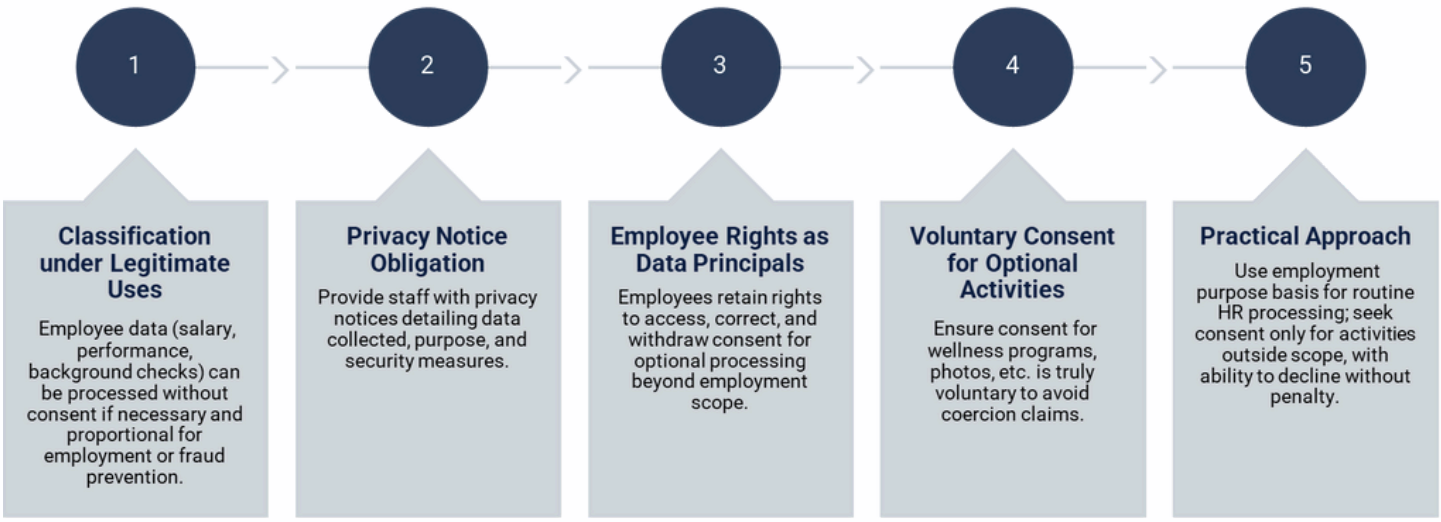
Customer Data Protection and Consent

NBFCs must provide clear, standalone privacy notices to borrowers and other customers, listing exactly what personal data is collected (e.g. identity details, financial information) and for what purpose.



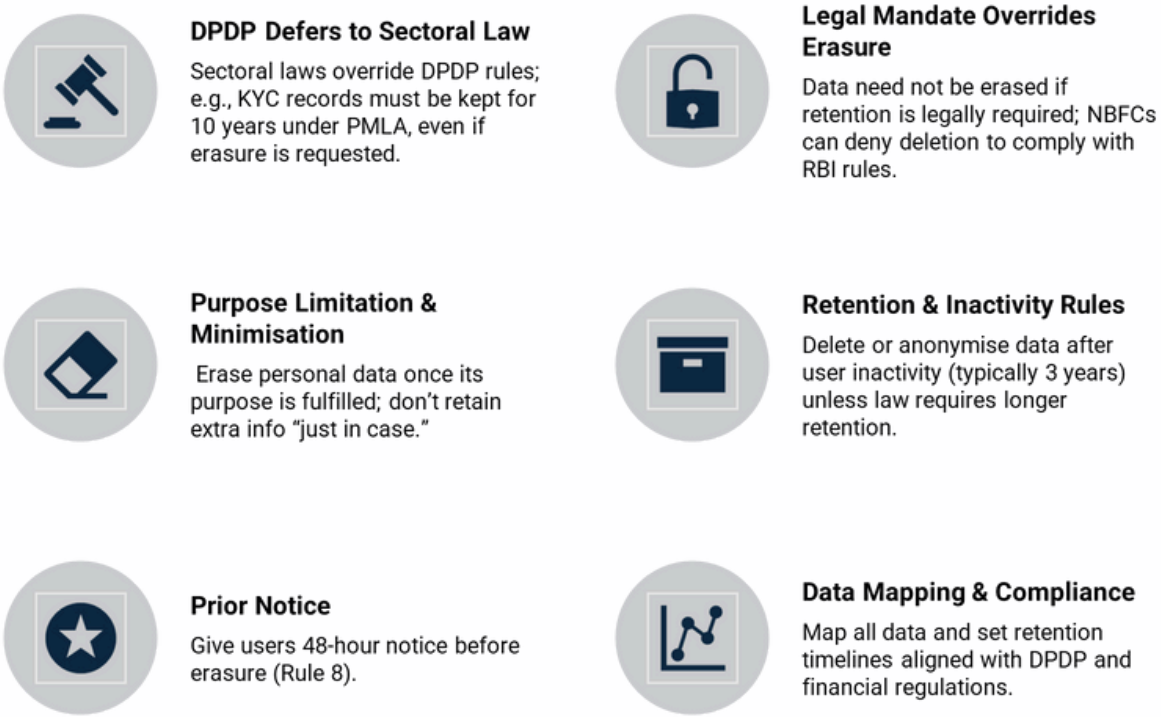
Internal Stakeholder Data (Employees and Partners)

The DPDP Act classifies employees' personal data under the "legitimate uses" exemption for employment purposes



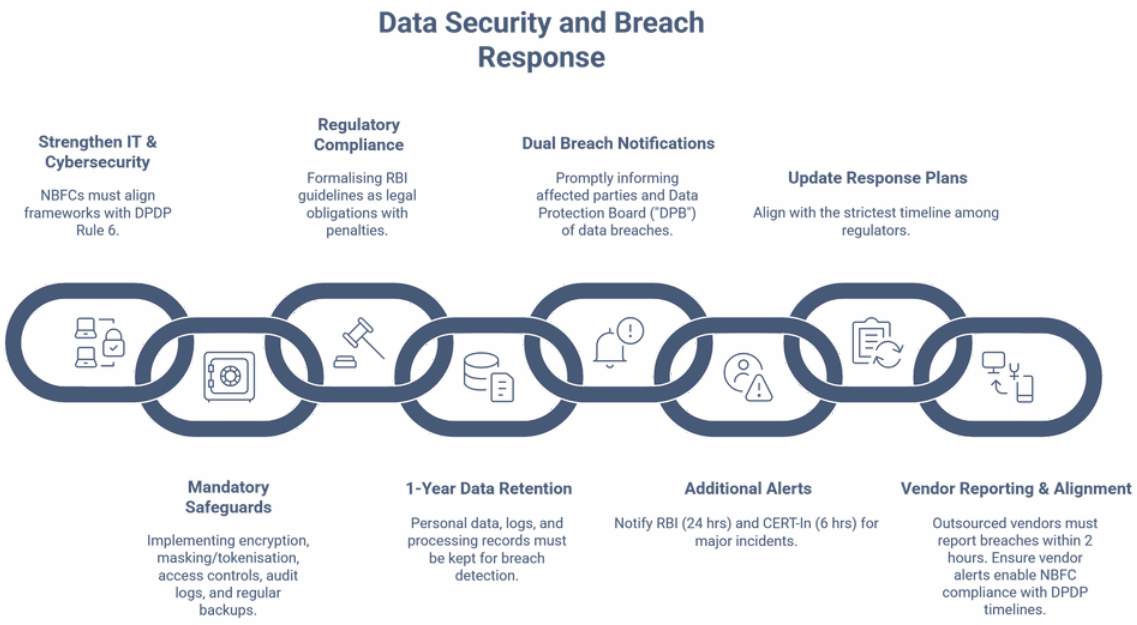
Regulatory Compliance vs. Data Deletion

NBFCs are already governed by RBI and other laws that mandate certain data handling practices. The DPDP rules explicitly defer to sectoral laws where necessary – for example, Know-Your-Customer (KYC) records must be retained for 10 years after an account is closed as per PMLA (anti-money laundering) rules, and this legal requirement overrides any individual's request to erase data earlier.



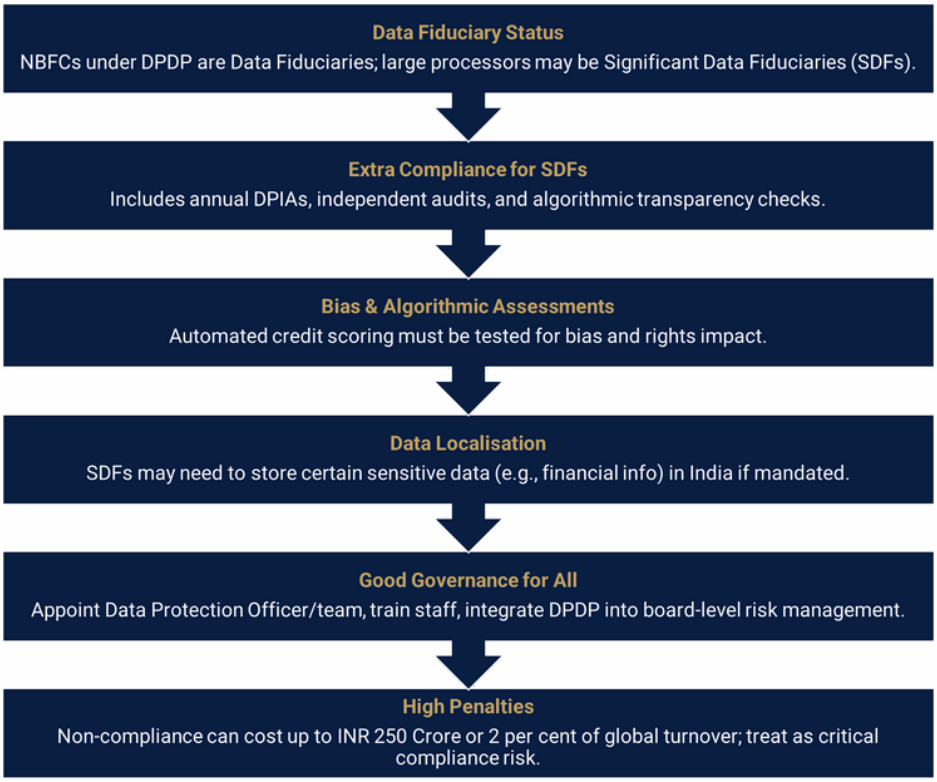
Data Security and Breach Response

NBFCs must bolster their IT and cybersecurity frameworks in line with Rule 6 of DPDP. Mandatory safeguards include encryption of sensitive data, masking or tokenisation of identifiers, strict access controls, audit logs, and regular data backups. Many NBFCs already follow RBI's IT security guidelines, but DPDP formalises these as legal obligations with penalties.



Data Governance and Accountability

Under DPDP, NBFCs will be considered Data Fiduciaries (or even Significant Data Fiduciaries if they process large volumes of personal data).



Credit Information and Algorithmic Use

One specific relief for NBFCs is that processing personal data for credit scoring and creditworthiness assessments is explicitly recognised as a “legitimate use” exemption under Section 17 of the Act. Section 17(4)(f) permits handling data without consent if “necessary to ascertain a borrower’s creditworthiness”.

Legal Basis

Section 17(4)(f) allows processing without consent for creditworthiness checks (e.g., Credit bureau reports, financial history).

Lawful Source

Data used must be lawfully obtained (e.g., Bank statements collected with consent or legal basis).

Document Exemption Use

NBCs should record when relying on this exemption and limit it to genuine credit checks.

Right To Correction

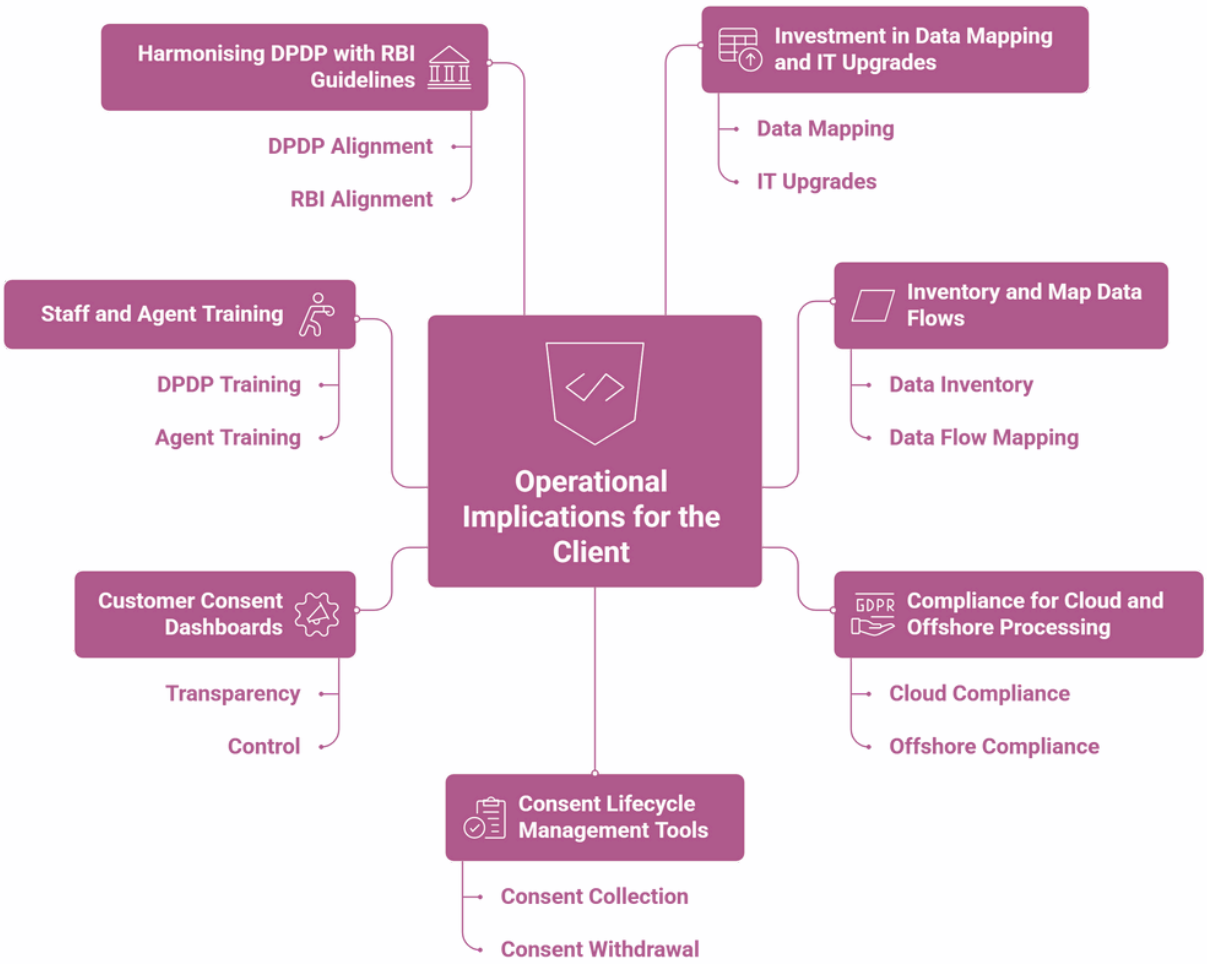
Data principals can demand correction of inaccuracies under DPDP and credit bureau rules.

Dispute Channels

NBCs must provide mechanisms for customers to dispute or correct data and link these to bureau processes.

Operational Implications

Complying with DPDP will require NBFCs to invest in data mapping and IT system upgrades.



- **Investment in Data Mapping**: Complying with DPDP will require NBFCs to invest in data mapping and IT system upgrades.
- **Inventory and Map Data Flows:** They should inventory all personal data they hold (customer, employee, partner data) and map data flows, including any cross-border transfers.
- **Compliance for Cloud and Offshore Processing: NBFCs** may have been using cloud services or offshore processing – under DPDP, therefore, they must ensure such processors enter into standard contractual clauses (SCCs) or agreements binding them to DPDP standards (including breach notification to the NBFC, confidentiality, etc.).

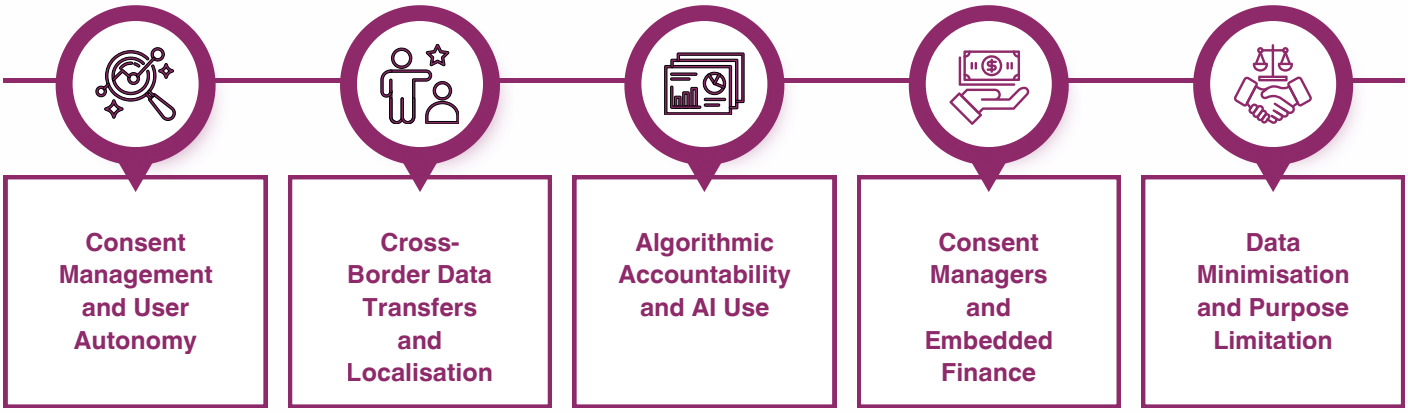
- **Consent Lifecycle Management Tools**: NBFCs will also need to build or integrate tools for consent lifecycle management – possibly leveraging emerging Consent Manager systems.
- **Customer Consent Dashboards:** For example, NBFCs could allow customers to manage consents via a central consent dashboard or through third-party Consent Manager platforms registered under DPDP (which will be available by 2026).
- **Staff and Agent Training:** Internally, NBFCs must sensitise their staff and agents: front-end teams should be trained to present privacy notices and handle customer data requests; IT teams must implement encryption and logging; compliance teams should prepare for timely breach reporting and interfacing with the DPB in case of complaints.
- **Harmonising DPDP Obligations with RBI Guidelines:** In summary, NBFCs faces a considerable compliance uplift, but many DPDP requirements align with existing financial-sector norms (e.g. RBI's localisation mandate for payments data and cybersecurity frameworks). NBFCs must proactively harmonise RBI guidelines with DPDP obligations – for instance, by layering new consent/rights management processes on top of their robust security and record-keeping systems – to mitigate duplication and ensure smoother compliance

Fintech Companies

A New Compliance Frontier for Fintech Companies

Fintech Companies

The FinTech sector, encompassing digital lending platforms, peer-to-peer lenders, wealth management apps, loan marketplaces, embedded finance services, etc., is directly affected by the DPDP Rules. FinTech firms often deal with highly personal financial data and innovative data uses (like alternative credit scoring, personalised investment advice), making DPDP compliance both crucial and challenging:

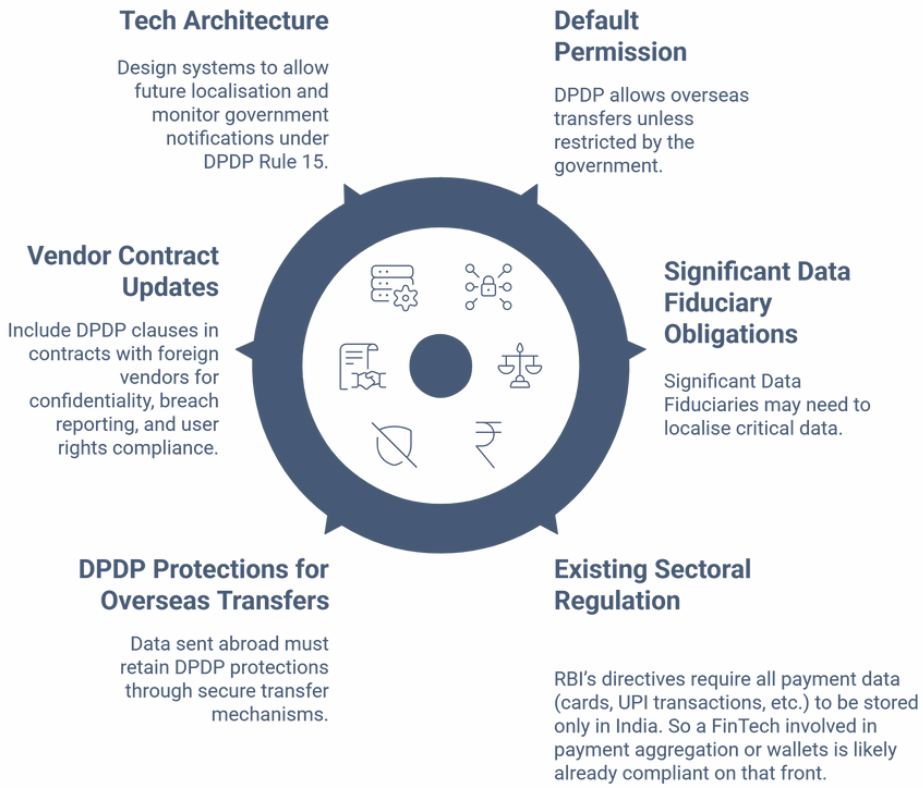


Consent Management and User Autonomy

FinTech companies must adopt a user-centric approach to data consent under DPDP. Traditionally, many fintech apps bundled consent into their terms of service or assumed consent for broad uses. Now, they are required to provide unbundled, specific consents for each purpose of data processing.

- **Specific Consent for Each Purpose**: Apps must seek separate explicit consent for every additional use beyond the primary purpose (e.g., marketing or partner data sharing).
- **Implementing Consent Management Systems (CMS):** FinTechs should deploy CMS for easy consent giving/withdrawal. They can integrate licensed Consent Managers or build Rule 4-compliant interfaces.
- **Key Obligations for FinTechs:** Provide a consent dashboard, enable one-click withdrawal, and maintain an auditable consent log.
- **Designing for Freely Given, Specific, Informed Consent:** Simplify privacy notices and redesign UX with clear, separate consent options for different data uses.
- **Competitive Advantage Through Transparency** :A well-designed Consent Manager dashboard can boost trust and differentiate fintech platforms.
- **Timeline for Compliance**: FinTechs should start aligning with this ecosystem early – the Rules allow one year (till late 2026) for the Consent Manager framework to kick in, but early adoption will smooth out integration issues.

Cross-Border Data Transfer and Localisation



Algorithmic Accountability and AI Use

FinTech innovation often involves algorithms – from credit scoring models and fraud detection systems to robo-advisors for investments. The DPDP Rules impose responsibilities to ensure that automated processing does not violate user rights or introduce bias/unfairness, especially for Significant Data Fiduciaries.

Annual Algorithmic Assessments for SDFs:

Significant Data Fiduciaries must audit AI models yearly for bias, explainability, and fairness.

Data Protection Impact Assessments (DPIAs):

SDFs must conduct DPIAs for new tech or large-scale sensitive data processing, documenting risks and mitigations.

Oversight by Data Protection Board:

Assessment reports can be requested by the Board, so compliance documentation is critical.

Voluntary Audits for Non-SDFs:

Non-SDF FinTechs should adopt privacy-by-design audits and certifications to demonstrate compliance.

Creditworthiness Exemption:

Credit scoring under Section 17 doesn't need separate consent, but accuracy and correction rights must be ensured.

Transparency and Contestability:

FinTechs should provide clear reasons for decisions and allow customers to contest them, aligning with global AI ethics.

Consent Managers and Embedded Finance

A unique challenge arises for embedded finance solutions – e.g., a fintech service embedded in an e-commerce app or a ride-hailing app offering credit. In such cases, user data flows from the main platform to the fintech provider.

1

Embedded Finance Data Sharing

In embedded finance (e.g., credit in e-commerce apps), both the main platform and fintech may act as independent Data Fiduciaries or Data Processor. They must disclose data sharing and obtain consent for specific purposes.

2

Consent for Specific Use Cases

If a wallet in a shopping app uses shopper data for identity verification or pay-later eligibility, explicit consent for that purpose is required.

3

Role of Consent Managers

Consent Managers provide a unified interface for managing consents across apps. India's Account Aggregator model is a similar concept under different regulations.

4

Interoperable Consent Frameworks

Upcoming DPDP Consent Manager networks will allow users to grant and revoke consent seamlessly across platforms.

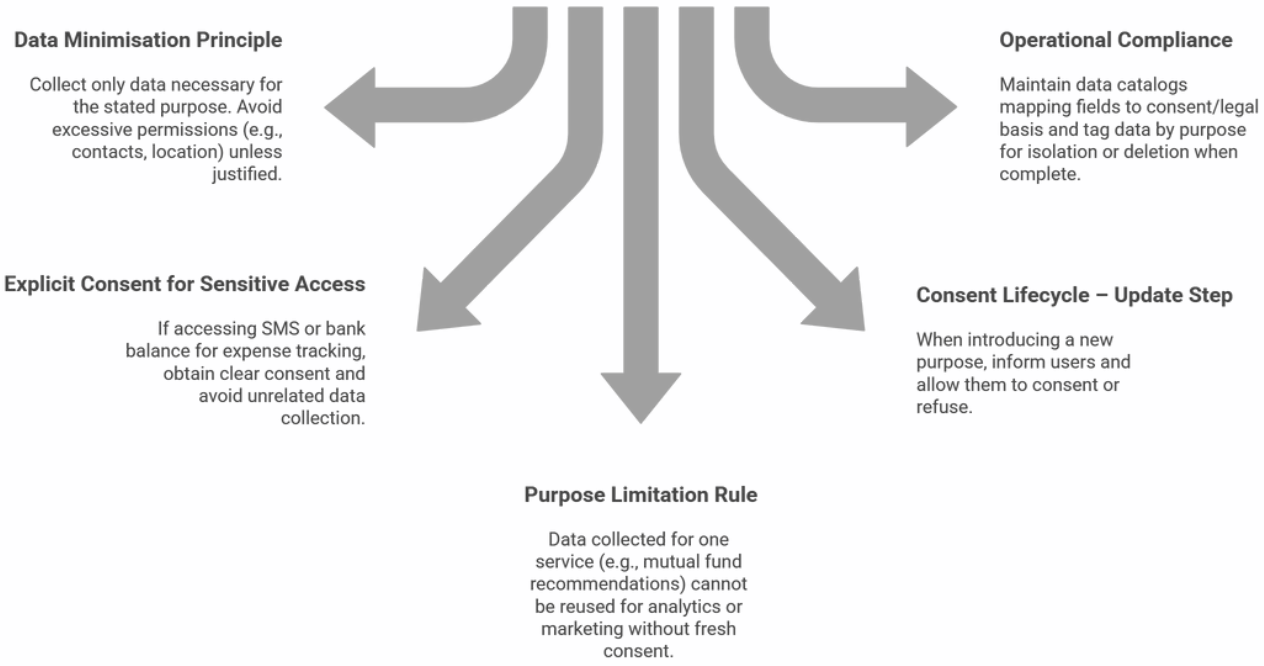
5

Technical Readiness

FinTechs should build API hooks and data architectures ready to integrate with standardised, interoperable consent frameworks.

Data Minimisation and Purpose Limitation

FinTech companies must re-examine their data collection practices. Under DPDP's data minimisation principle, only data required for the stated purpose should be collected and processed. Many fintech apps request extensive device permissions or personal details (contacts, location, etc.) – going forward, they will need to justify each piece of data.



Operational and Compliance Consideration for FinTech

Most FinTech companies are accustomed to a fast-paced, iterative development cycle. They will need to build compliance checkpoints into that cycle. Key steps include conducting privacy impact assessments during product design, implementing grievance redressal mechanisms for users (DPDP mandates that data principals be able to file complaints with the company easily and get timely resolution), and establishing a data protection oversight role (if not formally a DPO, at least a responsible manager).

Tech Solutions for Compliance

Use automated deletion tools for retention periods, encryption for data at rest/in transit, and consent preference centers in apps.

Multi-Regulator Alignment

Harmonizing sectoral rules with DPDP for consistent compliance.

User Education

Run user awareness programs on new privacy choices to build trust and turn compliance into a positive experience.

Industry Codes of Practice

Collaborative development of DPDP codes for FinTech.

Privacy as Core Design

Treat data privacy like security—integrate compliance into product architecture for long-term success.

Payment Systems and Prepaid Instruments

A New Era of Responsible Innovation for Payment Systems and Prepaid Instruments

Payment Systems and Prepaid Instruments

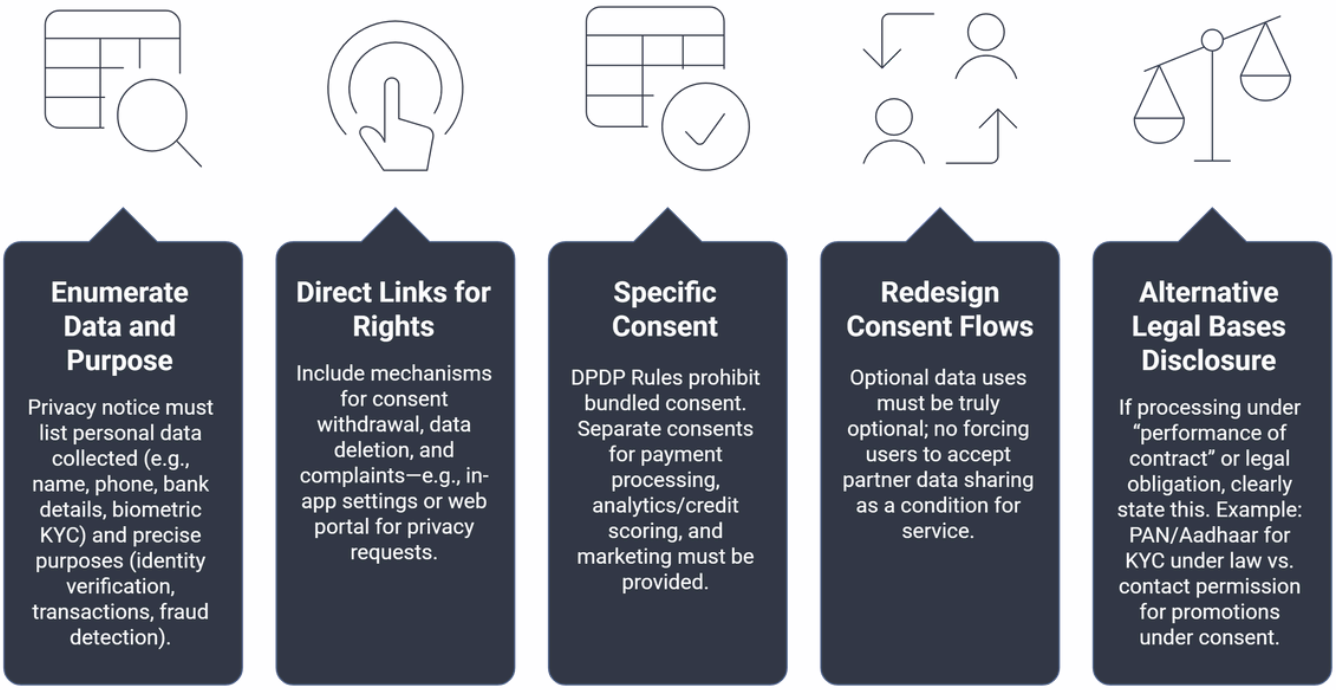
This sector includes payment gateway providers, payment aggregators, digital wallet issuers, prepaid card/e-wallet companies, and the entire ecosystem of issuers, acquirers, and payment processors. These entities handle transactional data and often sensitive financial information (like card numbers, UPI IDs, transaction histories). The DPDP Rules, 2025 impose specific duties that impact how payment services obtain consent, limit data use, and respond to incidents:

Consent Design and Transparency

Consent design in payment services must now be extremely clear and user-friendly. Many payment apps or wallet services traditionally bundled privacy consent with account opening. Under DPDP, they must present a standalone privacy notice (separately from terms of service) at or before data collection.

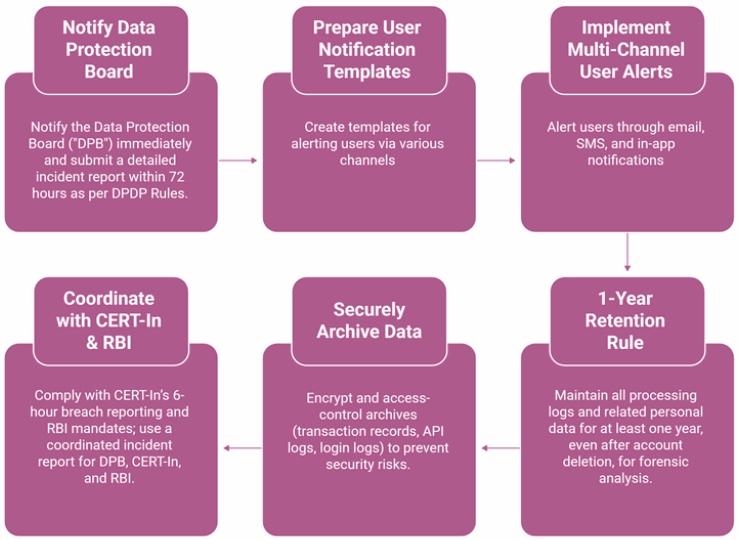
Purpose Limitation in Data Use

Payment service providers are expected to adhere to purpose limitation strictly. They typically collect data to complete transactions and prevent fraud – those are permissible uses. However, many might be tempted to leverage transaction data for additional gains (like monetising spending patterns or cross-selling financial products).



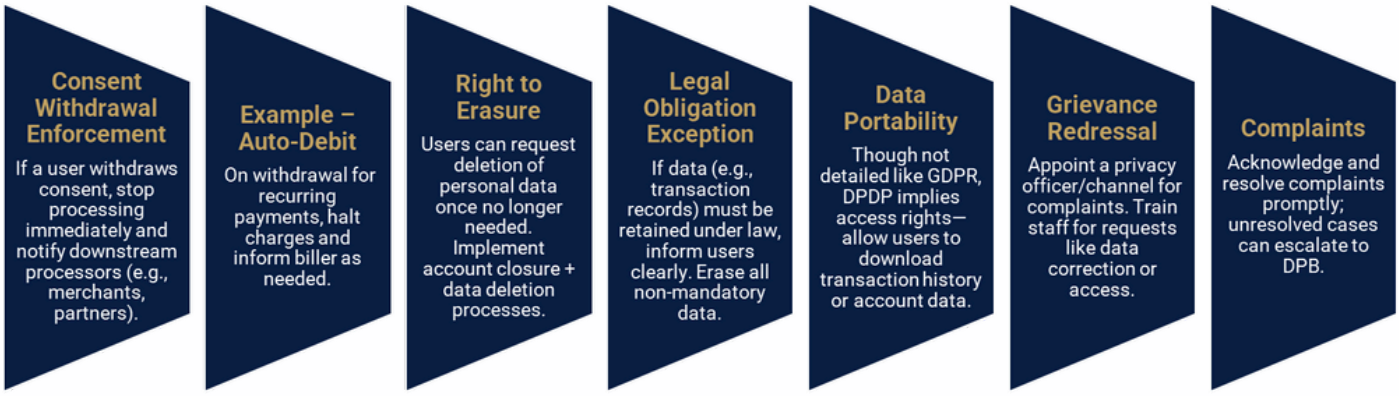
Breach Notification and Incident Management

Given the sensitivity of financial data, the breach notification rule (Rule 7) is vital for payment systems. If a security incident occurs (for instance, a leak of cardholder data or wallet account info), the provider must immediately notify all affected users, detailing the nature of personal data compromised, potential consequences, and steps they should take (like resetting passwords).



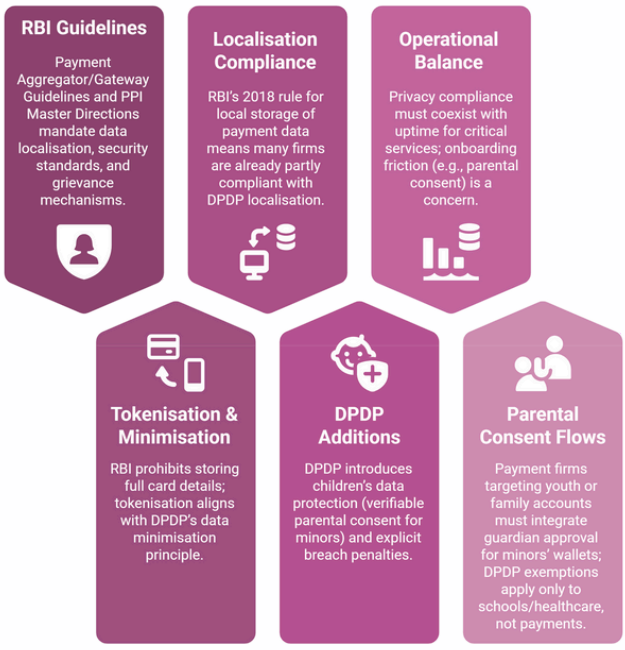
User-Friendly Withdrawal and Data Rights

The concept of "frictionless withdrawal" of consent is particularly emphasised for consumer-facing services like payments. In practical terms, a wallet or payment app should allow users to easily revoke permissions – for instance, turning off data sharing with third parties or withdrawing consent for saved card details.



Integration with Existing Financial Regulations

Payment and PPI providers should reconcile DPDP with the RBI's regulations on payments.



Operational Strategies for Payment Sector

Payment system providers should undertake a data flow audit – mapping from the point a user initiates a payment or KYC, through the processing (acquirer, network, issuer), to storage and subsequent uses. Every point where personal data is touched should be evaluated for compliance: is there a valid consent or legal need? is the data encrypted? is it logged?

Review Merchant Plug-ins
Ensure plug-ins capturing customer info comply with DPDP notice standards.

Consent Screens & Languages
Update consent screens for specific purposes; provide in multiple languages for "informed" consent.

Define Roles in Data Chain
Clearly assign Data Fiduciary vs Data Processor roles among merchants, gateways, banks; update contracts for consent withdrawal compliance.

Test Consent Withdrawal
DPDP requires withdrawal to be as easy as giving consent. Implement toggles and verify backend stops related processing.

Breach Reporting Drills
Prepare for 72-hour DPB reporting; simulate leaks and coordinate with CERT-In and RBI for unified incident response.

1-Year Log Retention
Set up secure log management for processing logs and personal data retention per DPDP; encrypt and access-control archives.

Invest in Security Tools
Deploy intrusion detection and data loss prevention systems to meet RBI and DPDP expectations.

Build Trust Through Compliance
Clear consent flows and easy opt-outs reduce user concerns; long-term benefit is a transparent, low-risk ecosystem.

Healthcare Systems

A New Privacy Mandate for Healthcare Systems

Healthcare Sector

The healthcare sector – including private hospitals, clinics, telemedicine platforms, health insurance providers, and government health schemes like Ayushman Bharat – handles some of the most sensitive personal data (health and medical information). The DPDP Act and Rules apply to digital personal health data and introduce protections balanced with certain exemptions to ensure healthcare delivery isn't hampered. Key implications for this sector are:

Strengthened Patient Data Privacy

Hospitals and health-tech companies are now clearly recognised as Data Fiduciaries when processing patient data. They must institute robust privacy practices for handling health records, medical test results, insurance details, etc.

1. Privacy Notice at Data Collection
Provide notice to patients/guardians during registration or telemedicine sign-up, detailing personal health data collected and its purposes (treatment, billing, research).

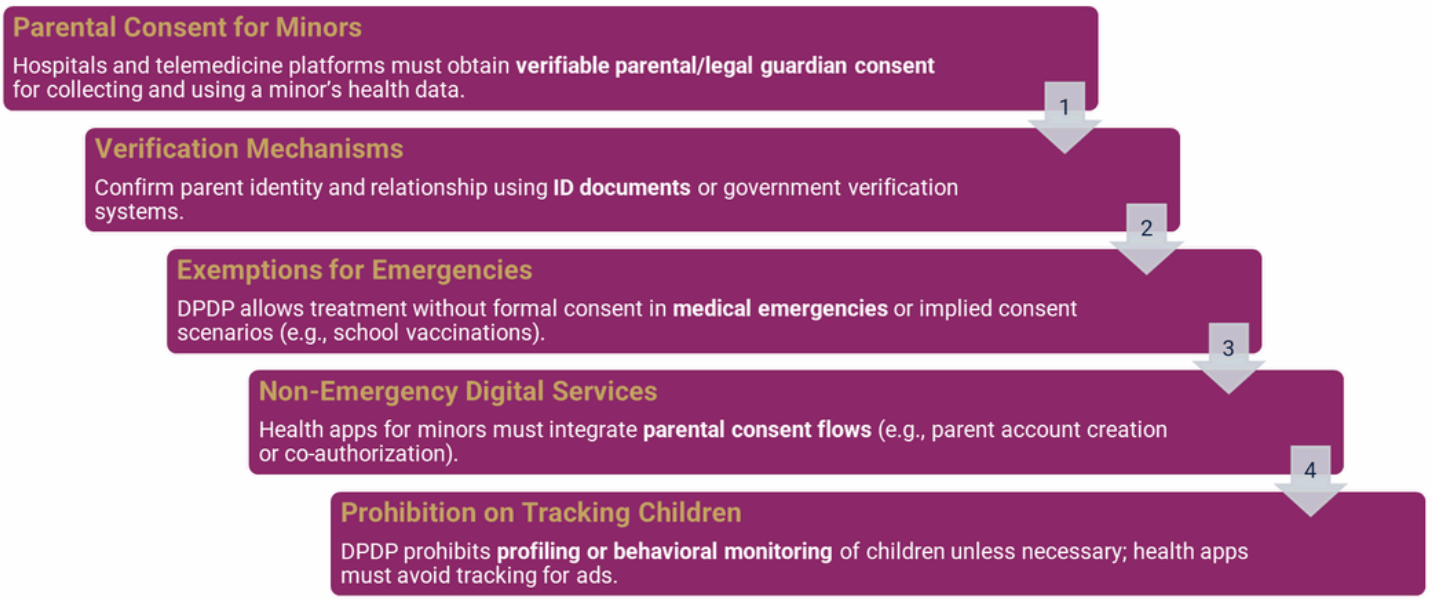
2. Explain Data Sharing Clearly
Use plain language to disclose sharing with labs/specialists for treatment (implied consent) and seek separate consent for optional uses like research or marketing.

3. Data Minimisation Principle
Collect only data relevant to care. Review intake forms and app permissions to remove unnecessary fields.

4. Justify Sensitive Permissions
If collecting location or contacts, ensure a valid purpose (e.g., emergency contact, nearby labs) and obtain explicit consent.

Verifiable Parental Consent for Minors

Healthcare often deals with data of children (e.g. pediatric care). The DPDP Rules mandate verifiable parental (or guardian) consent for any data processing of children under 18.



Exemptions for Health-Related Processing

The DPDP Act acknowledges that certain health scenarios warrant processing without the delays of consent. Section 7(5) of the Act permits processing personal data without consent in a "medical emergency" where obtaining consent is not practicable. This would cover unconscious patients brought to ER, disaster situations, etc.

Data Retention and Deletion Practices

Healthcare providers must align their record retention policies with DPDP's rules while respecting medical record regulations. Typically, hospitals maintain patient records for a certain period due to medical, legal, or regulatory reasons.

Erasure Rule

Personal data must be erased once no longer needed, unless retention is required by law.

Statutory Retention Requirements

Healthcare laws override DPDP erasure—e.g., Clinical Establishment Rules:

In-patient case records: 3 years

Radiology films: 5 years

Telemedicine recordings: 30 days

Document Legal Obligations

Hospitals must record retention mandates (Medical Council, Atomic Energy, etc.) to justify non-erasure under DPDP.

Post-Retention Deletion

After statutory period, delete or anonymise records. Implement automated retention schedules in IT systems.

Mandatory Log Retention

Keep processing logs for 1 year even after data deletion for audit and breach investigations; logs must be secure and minimal.

Breach Response in Healthcare

Healthcare data breaches can be extremely sensitive (exposing diagnoses, HIV status, etc.), so DPDP's breach notification requirements take on special significance. Hospitals and clinics must have in place a protocol to detect and report breaches. If, say, a laptop with patient records is stolen or a health app's database is hacked, the entity must notify the affected patients promptly and also inform the Data Protection Board within 72 hours with a report.

Notification Details

Include nature of data breached (e.g., medical test results), implications, and user actions (e.g., reset password, beware phishing).

Sector-Specific Escalation

If breach involves government health schemes (e.g., Ayushman Bharat), inform relevant authorities.

CERT-In Coordination

Comply with CERT-In's 6-hour cyber incident reporting rule alongside DPDP requirements.

Penalties for Non-Compliance

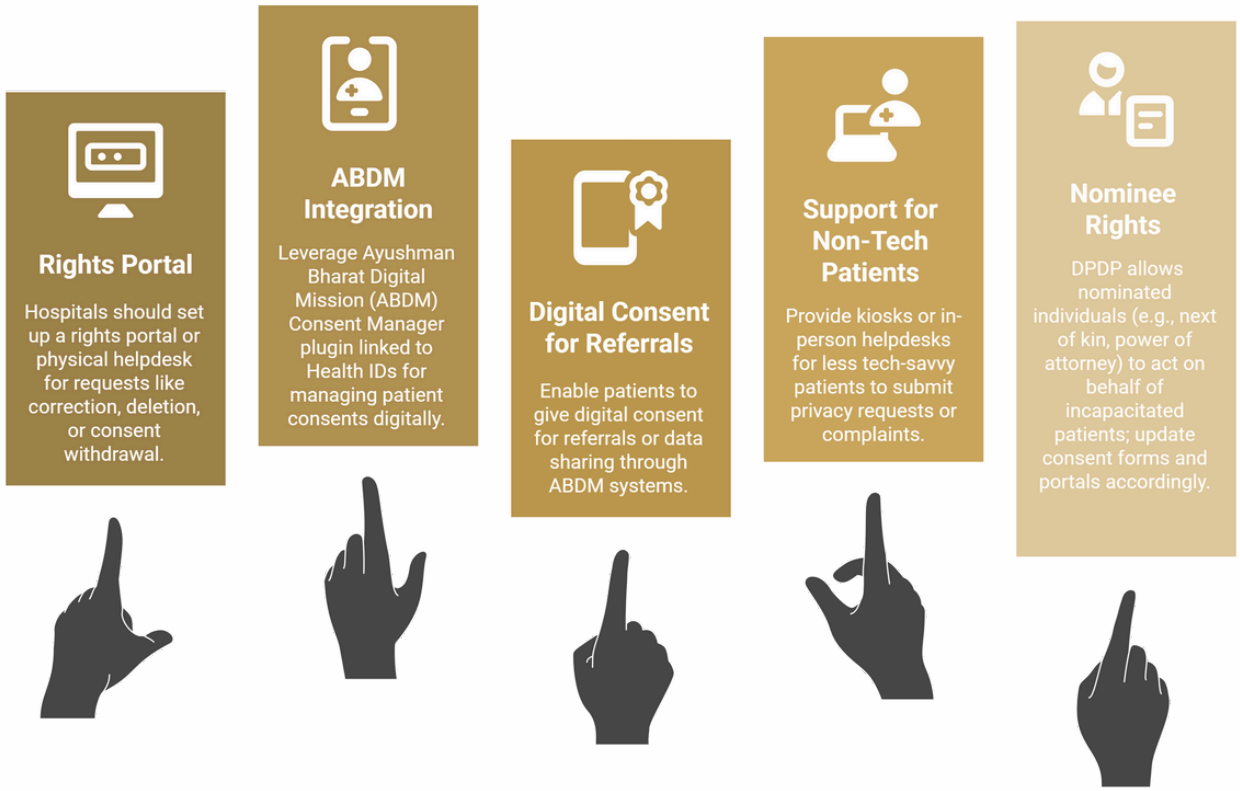
Failure to notify breaches under DPDP attracts explicit penalties—under-reporting is risky.

Preparedness & Drills

Run breach response drills (e.g., ransomware scenarios) to ensure timely compliance with DPDP timelines.

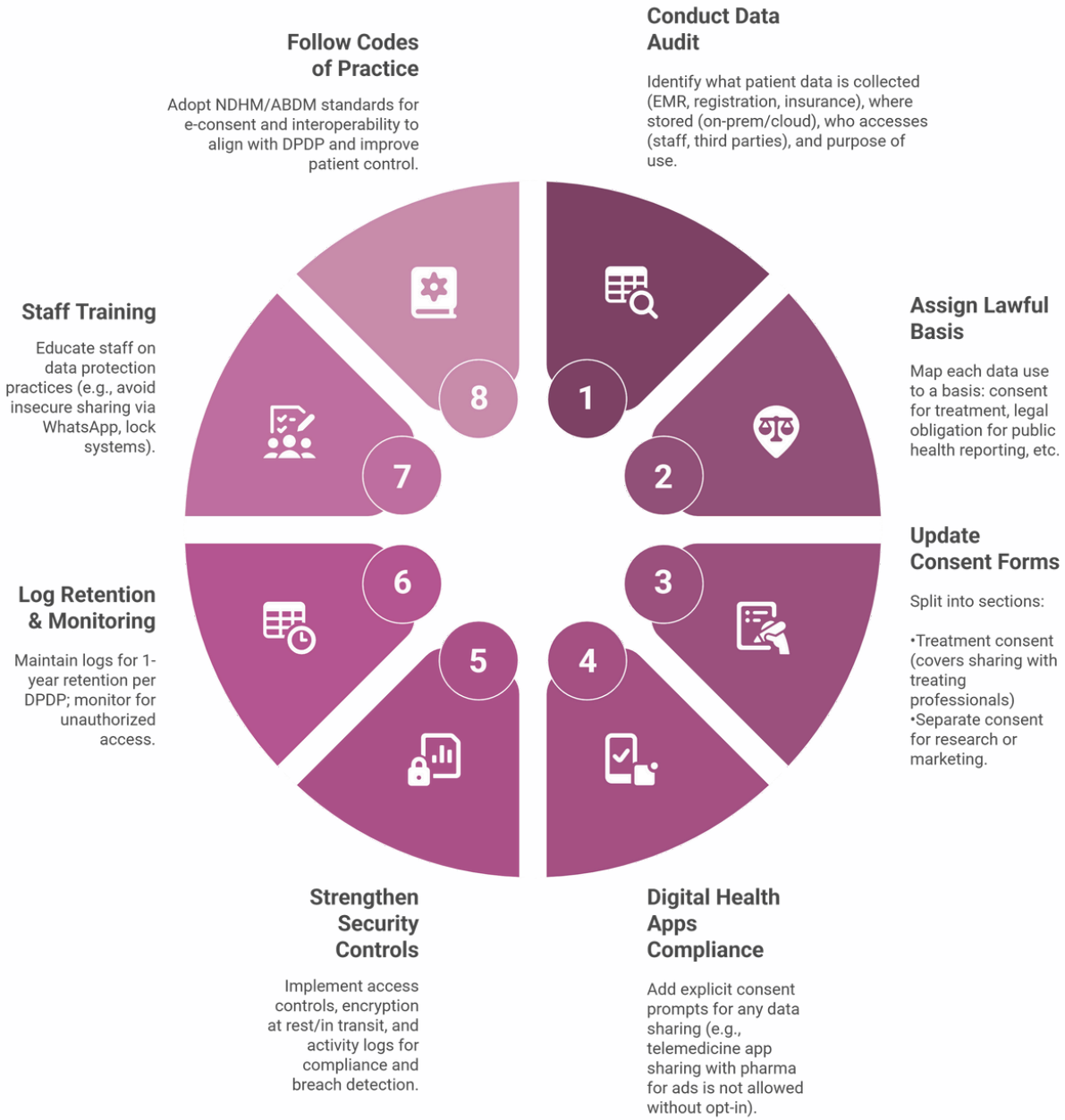
Implementing User Rights and Grievances

Healthcare providers need to set up ways for patients to exercise their data rights without hindering care. Under DPDP, patients (data principals) have the right to access their records, correct inaccuracies, and even have data deleted when appropriate. Many hospitals already allow patients to request copies of their reports or discharge summaries – this will now be a legal right.



Operational Challenges and Recommendations for Healthcare

Healthcare entities often use a mix of digital and physical records. DPDP technically covers digital personal data, which includes data initially collected non-digitally but later digitised. Hospitals should accelerate digitisation (if not already) to manage compliance uniformly.



Cross-Sector Impacts and Strategic Recommendations

Cross-Sector Impacts and Strategic Recommendations

Implementing the DPDP Rules, 2025, is a substantial endeavour across all sectors. While each sector faces unique scenarios, several common themes emerge:

Overhaul of Internal Systems and Architecture	Data Governance and Accountability	Security Measures and Risk Management	Grievance Redressal and Consumer Communication
Map all systems storing personal data, tag by purpose and consent status, enable segregation/deletion, and extend log retention to 1 year (Rule 8(3)). Implement encryption, tokenisation, and Consent Management Platforms for unified consent tracking. Legacy systems should be upgraded or replaced; consider cross-functional IT & compliance taskforce for phased rollout (major provisions effective by 2027).	Strengthen governance by appointing a Data Protection Officer or committee, creating policies for data handling and sharing, and training staff. Maintain DPIA reports, consent records (7+ years for Consent Managers), and processing logs. Prepare for DPB audits and monitor sectoral guidelines (RBI, IRDAI, NHRA) for dual compliance. Conduct internal audits and gap assessments regularly.	Adopt encryption, pseudonymisation, access control, and breach monitoring. Apply risk-based protection for sensitive data (financial info, health records). Update incident response plans for 72-hour DPB reporting and run breach drills. Perform DPIAs for high-risk projects and enforce vendor contracts with DPDP Standard Contractual Clauses and breach obligations. Audit vendors for compliance.	Set up a privacy grievance mechanism (portal/email/helpdesk) with clear SLAs for acknowledgement and resolution. Enable workflows for data access, correction, deletion, and notify third parties. Update privacy policies and FAQs for transparency, clarifying legal retention exceptions (e.g., RBI transaction record rules). Clear communication fosters trust in sensitive sectors like finance and healthcare.

Sector-Specific Adjustments

While DPDP is a horizontal law, each sector should interpret it in context of its domain:

Financial services (Banks/NBFC/Fintech)

Align DPDP with RBI digital banking guidelines. Create a compliance matrix mapping DPDP provisions to existing programs (cybersecurity, KYC/AML). Use RBIs in frameworks for DPDP security and customer communication channels for DPDP rights.

Payments

Integrate DPDP consents into mandate systems. Design UI/UX to show data protection indicators. Collaborate with NPCI for standard consent templates.

Healthcare

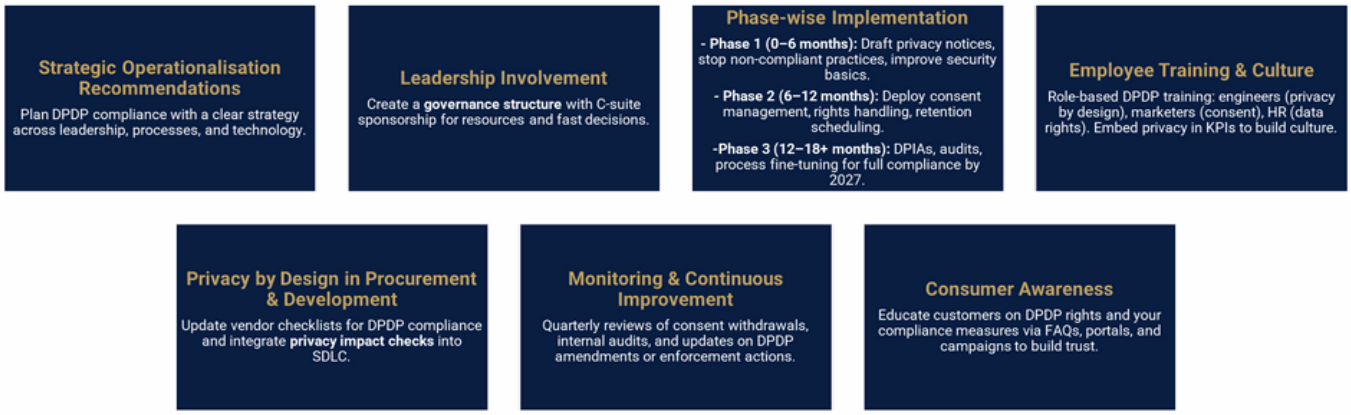
Work with regulators for consent exemptions or simplified consent for routine care. Implement one-time dpdp-compliant treatment consent. Ensure fallback for emergencies under section 7 exemptions.

All sectors

Assess significant data fiduciary (SDF) status. If near threshold, adopt SDF-level compliance early—DPIAS, audits, risk assessments—to reduce exposure and prepare for designation.

Strategic Operationalisation Recommendations

To effectively operationalise DPDP compliance across the organisation, consider the following strategy:



Conclusion

In conclusion, the DPDP Rules, 2025 compel businesses across NBFC, FinTech, Payments, and Healthcare to elevate their data protection practices to a new standard. While compliance demands significant effort – from technical upgrades to policy reforms – it ultimately mitigates risks (legal and reputational) and aligns with a global trend towards stronger data privacy. By taking a sector-tailored but principle-driven approach, organisations can not only meet the letter of the law but also build trust with consumers through robust privacy and security measures. Each sector must integrate these rules with its operational realities, but the overarching goal remains common: safeguarding individuals' digital personal data and treating privacy as a core organisational value.

Contact us

Ground Floor, 27-A, Hauz Khas Village,
New Delhi, 110016
Office: +91 11 41727676
info@akandpartners.in
www.akandpartners.in

