ADVOCATES & SOLICITORS

SWITCHING ON DPDP

AN IMPLEMENTATION GUIDE TO THE 2025 RULES

Prepared By

AK & Partners

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

All hands-on-board with the new DPDP Rules. If you think there is a lot of time, think again. To comply with the new Rules effectively, companies should adopt a risk-based approach to security. This means identifying your "crown jewel" data – the most sensitive or mission-critical personal data you hold (for example, in a fintech this might be financial transaction data and KYC details; in a hospital, patient health records; in an e-commerce, payment info and addresses) – and applying extra layers of protection to those assets.

Perform periodic security risk assessments to evaluate threats and vulnerabilities in systems and processes. It's wise to bring in independent experts or use standards (like ISO 27001, or conduct SOC2 audits) to benchmark your security. Regular audits (internal or external) should check that the required controls (encryption, access control, logs, etc.) are not just in place on paper but working in practice – e.g., test whether you can retrieve audit logs for a given period, verify backups by doing test restores, ensure user access rights are reviewed and recertified periodically.

Organizations should update their incident response plan to align with DPDP's breach reporting timeline. This involves defining clear roles (IT, legal, compliance, communications) when a breach hits, and practicing it. Running drills or tabletop exercises – for example, simulating a ransomware attack to see if your team can detect it, shut down systems, assess impact, and draft notifications all within 72 hours – is extremely useful. These drills can reveal gaps (maybe backups weren't working, or legal review of notices took too long) which you can fix before a real incident occurs.

Finally, many firms find it helpful to obtain security certifications or undergo external audits not just for compliance but to build trust (especially if you're a service provider). Under DPDP, demonstrating due diligence in security can also be a mitigating factor against penalties in case something does go wrong. In summary, Rule 6 pushes companies to elevate their security housekeeping to a consistent, documented, and verifiable standard – integrating security into procurement (vendor contracts), project design, daily IT operations, and corporate governance. For most, this formalizes what might already be best practices, but given the rising cyber threats, it ensures organizations keep security front-and-center.

Each of these new obligations under the DPDP Rules, 2025 – from better consent notices to breach reporting and special protections for children, to higher standards for significant data handlers and baseline security – will require companies to review and update their compliance strategies. Compliance officers and legal teams should translate these rules into actionable checklists and work closely with product, IT, and business owners to implement changes. The emphasis is on transparency, accountability, and user empowerment in data processing. By addressing these areas proactively (e.g. redesigning consent forms, setting up incident-response drills, identifying SDFs), organizations can not only meet the legal requirements by the 18-month deadline, but also build greater trust with their customers and stakeholders in the long run.

Awards & Recognitions

Scope

This Report provides a practical, business-focused guide to the Digital Personal Data Protection Rules, 2025 (DPDP Rules), and their interaction with the Digital Personal Data Protection Act, 2023, for organisations operating in or targeting India. It is designed for in-house legal, compliance, risk, technology, and product teams that must translate the new framework into concrete implementation steps.

Research Methodology

The analysis in this Report is grounded in a close reading of the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 as notified, including implementation timelines, rule-by-rule obligations, and related schedules. Review of relevant allied instruments and guidance (such as CERT-In directions, sectoral record-keeping norms, and emerging government communications on appointments and governance of the Data Protection Board) to identify overlaps and interaction points.

Executive Summary

The DPDP Rules, 2025 operationalise the DPDP Act, 2023 by specifying how organisations must obtain consent, secure personal data, respond to breaches, and handle high-risk processing. First, the implementation calendar staggers obligations but does not leave a long runway. While certain elements, such as registration of Consent Managers, have specific future dates, others, including the functioning of the Digital Data Protection Board – commence immediately. Secondly, the Rules re-set how consent and transparency must work in practice. Notices now need to be standalone, plain-language, and itemised by data category and purpose, with granular opt-ins and easy withdrawal. Dual notification of personal data breaches, to affected individuals and to the Board within a staged, 72-hour framework, removes “no-harm” thresholds and demands tested incident-response playbooks. Thirdly, the Rules impose heightened duties around vulnerable groups and high-impact processing. Processing data of children and certain persons with disabilities requires verifiable parental or guardian consent, subject to narrow exemptions for essential services. Organisations that are to be designated as Significant Data Fiduciaries must prepare for annual DPIAs & independent data audits. Across all Data Fiduciaries, security safeguards are now codified, including encryption, access control, and one-year minimum security-log retention, supported by business-continuity and recovery capabilities.

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		

The Digital Data Protection Board

DIGITAL OFFICE FOR DIGITAL PERSONAL DATA

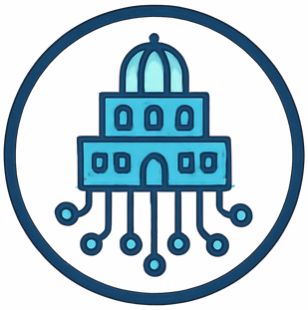
The Data Protection Board of India is a fully virtual, paperless quasi-judicial body for digital personal data.

WHO IS THE DATA PROTECTION BOARD OF INDIA?

A central adjudicatory body for digital personal data issues. Headed by a Chairperson, supported by Members and staff. Functions as a quasi-judicial authority for data protection.

HOW DOES THE BOARD FUNCTION?

Meets entirely through virtual/video-conference platforms. Issues orders, notices, and directions digitally. Conducts inquiries and hearings using electronic records.



WHAT MAKES THE BOARD UNIQUE?

Designed as a fully digital office, not a traditional department. Has no fixed physical office location. Built to be technology-enabled and paperless by design.

TECHNO-LEGAL PROCEEDINGS OF THE BOARD AND APPELLATE TRIBUNAL

Secure, digital proceedings with the same legal value as in-person hearings.

WHAT ARE "TECHNO-LEGAL MEASURES"?

- Use of validated technological tools in legal proceedings.
- Same evidentiary value as physical appearance before courts/tribunals.
- Intentionally broad term – Rules do not fix specific technologies

HOW DO THEY WORK IN PRACTICE?

Appearances: Any person summoned or required to appear before the Board may do so using secure, validated digital tools.

Hearings & Filing: Hearings, pleadings, filings, and records can be conducted and managed through digital platforms.

Evidence and Orders: Evidence and orders are handled electronically with the same legal effect as physical documents.

WHERE DO TECHNO-LEGAL MEASURES APPLY?

Data Protection Board

Functions as a digital office. Uses techno-legal measures for appearances, hearings, evidence, and orders.

Appellate Tribunal

Functions as a digital office. Adopts techno-legal measures for hearings, filings, evidence, and orders.

NOTES FOR GOVERNMENT RELATIONS – SEARCH COMMITTEE

The Government has formally initiated the search for the Chairperson and Members of the Data Protection Board of India.

STATUS OF APPOINTMENTS

The search for the Chairperson and Members of the Data Protection Board of India is officially underway. A high-level committee has been constituted to identify and recommend suitable candidates.

COMPOSITION OF THE SEARCH COMMITTEE

Cabinet Secretary (name yet to be disclosed).
Secretary, Ministry of Electronics and Information Technology – currently Shri S. Krishnan.
Secretary, Department of Legal Affairs – currently Dr. Anju Rathi Rana.
Two experts with proven expertise in data protection, cybersecurity, technology regulation, or allied domains.

RECOMMENDATION MECHANISM

The Members of the Board will be recommended by:
Secretary, Ministry of Electronics and Information Technology;
Secretary, Department of Legal Affairs;
The two domain experts on the committee;
The Cabinet Secretary is part of the search committee but does not participate in the recommendation of Members.

KEY TAKEAWAY

Engagement will primarily centre around the two Secretaries and the two experts, who jointly recommend Board Members. The Cabinet Secretary's role is institutional and supervisory, not directly involved in candidate recommendation.

Consent Notice Requirements

Under Rule 3, any request for consent shall be accompanied by a clear and standalone privacy notice for the Data Principal (the individual). The DPDP Rules introduce a stricter format and content for these notices.

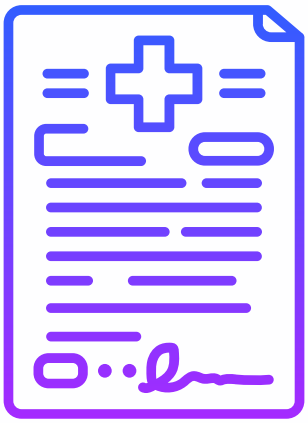
INDEPENDENT & PLAIN LANGUAGE

Shown separately from other terms and conditions.

Not buried inside lengthy T&Cs or privacy policies.

Written in clear, simple language.

Understandable on its own, without needing other documents.



ITEMIZED DATA AND PURPOSE

Explicitly lists each category of personal data collected.

Clearly states the specific purpose(s) for processing each category.

Explains what service or functionality is enabled by that processing.

Rejects generic, blanket consents like “we may use your data for various purposes”.

CONSENT OPTIONS & WITHDRAWAL

Allows users to accept or decline each purpose separately (granular consent).

Optional uses (e.g., marketing) are not tied to core service access.

Provides an easy mechanism (links/buttons) to withdraw consent and exercise data rights.

Explains how to lodge a complaint with the Data Protection Board (DPB).

Withdrawing consent is as simple as giving it (no complex, multi-step process).

PRACTICAL EXAMPLE – LENDING APPS & ONBOARDING FORMS

- For example, a digital lending platform's signup form will now include a dedicated privacy notice listing the personal data it collects (e.g. name, contact, PAN, salary, bank statements) and the purpose for each: KYC verification, credit risk assessment, loan servicing, etc.

- Each purpose would have its own consent checkbox.

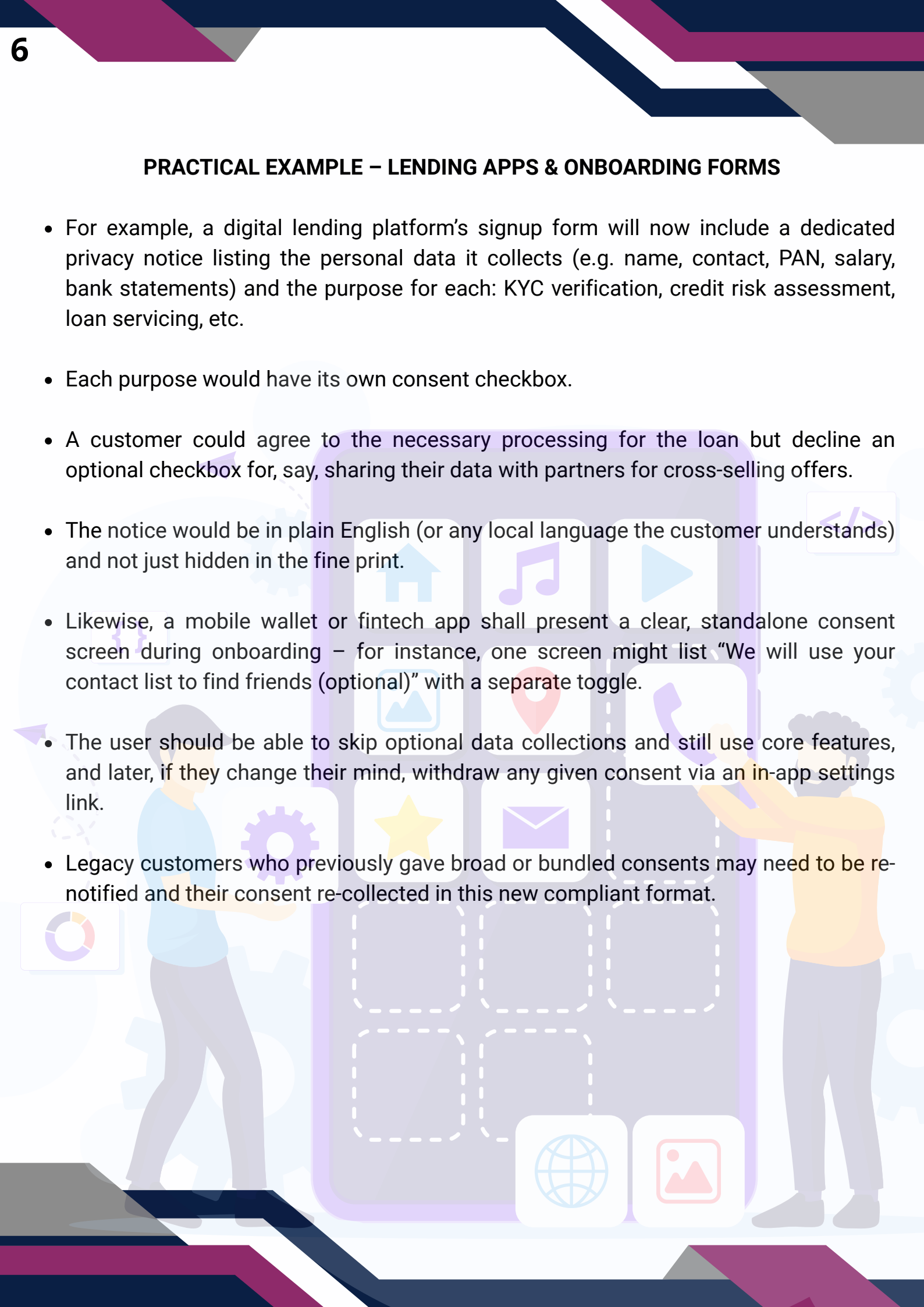
- A customer could agree to the necessary processing for the loan but decline an optional checkbox for, say, sharing their data with partners for cross-selling offers.

- The notice would be in plain English (or any local language the customer understands) and not just hidden in the fine print.

- Likewise, a mobile wallet or fintech app shall present a clear, standalone consent screen during onboarding – for instance, one screen might list "We will use your contact list to find friends (optional)" with a separate toggle.

- The user should be able to skip optional data collections and still use core features, and later, if they change their mind, withdraw any given consent via an in-app settings link.

- Legacy customers who previously gave broad or bundled consents may need to be re-notified and their consent re-collected in this new compliant format.



Next Steps for Consent Notice

- Catalogue all personal data processed, purpose, and retention periods.
- Classify lawful basis: consent, contract, legal obligation, etc.
- Verify that non-erasable data (e.g. statutory records) is appropriately flagged.

LAW	MINIMUM RETENTION PERIOD
Income Tax Rules, 1962 – Rule 6F(5)	6 years from the end of the relevant assessment year.
Companies Act, 2013 – Section 128(5)	Not less than 8 financial years immediately preceding the current year; longer if any investigation is ordered (books relevant to investigation to be kept for the period specified in the order).
Central Goods and Services Tax Act, 2017 – Section 36	Until expiry of 72 months from the due date of furnishing of annual return for the year; if under appeal / revision / investigation, books for those periods must be kept for 1 year after final disposal, or the 72-month period, whichever is later.
Prevention of Money-laundering Act, 2002 – Section 12(3) & 12(4)	(a) 5 years from the date of transaction for transaction records; (b) 5 years after the business relationship has ended / account closed for client-identification and related records.
RBI Master Direction – Know Your Customer (KYC) Direction, 2016 (as amended), para 46	(a) At least 5 years from the date of transaction for transaction records; (b) At least 5 years after end of business relationship for identification / address records.

LAW	MINIMUM RETENTION PERIOD
CERT-In Directions dated 28 April 2022 (under IT Act)	Logs: all ICT system logs (as specified) must be retained for a rolling period of 180 days in India. Customer / transaction data for certain entities (VPN, cloud, VASPs etc.): to be retained for 5 years or longer as required by law even after cancellation / withdrawal / expiry of registration or contract.
Securities and Exchange Board of India (Stock Brokers) Regulations 1992 - Regulation 18	Every stock broker shall preserve the books of account and other records maintained for a minimum period of 5 years.
IRDAI – Revised Guidelines on Insurance Repositories and Electronic Issuance of Insurance Policies, 29 May 2015 – clause 18	Minimum 10 years from the date of cancellation of the contract; policies with outstanding claims or under litigation must be held 10 years from date of settlement / closure of litigation.
IRDAI (Insurance Brokers) Regulations, 2018 – Regulation on "Books of account, records and documents" (reg. 33(5))	At least 7 years from the end of the year to which the records relate; for cases where claims are reported and decision pending in court, documents must be kept till disposal by the court, and for some reinsurance documents, till their natural expiry.

Dual Notification Obligation for Data Breach

DUAL NOTIFICATION FOR PERSONAL DATA BREACH
Rule 7 – DPDP Rules

BREACH DETECTED

Organisation becomes aware of any personal data breach

NOTIFY AFFECTED INDIVIDUALS

Timing: Without undue delay

- Inform all impacted Data Principals as soon as the breach is detected.
- Use clear, simple language to explain what happened and which personal data may be affected.
- Describe key risks (for example, identity theft or financial fraud) in plain terms.
- Provide practical steps individuals can take to protect themselves.
- Use channels that reach users quickly (for example, email, SMS, in-app alerts).

NOTIFY DPB

- Initial intimation: Send an early notification to the DPB without delay.
- Share basic facts: nature of the breach, suspected scope, and likely impact.
- Indicate when the incident was detected and, if known, when it occurred.
- Detailed report (within 72 hours): Submit a fuller breach report to the DPB within 72 hours of initial intimation.
- Cover the root cause, categories of data involved, and number of Data Principals affected.
- Set out mitigation measures taken and longer-term remediation plans.
- Confirm that affected individuals have been informed and summarise what they were told.

Rule 7 of the DPDP Rules imposes a dual, timeline-bound notification framework whenever a Data Fiduciary becomes aware of any personal data breach. This framework requires the organisation to promptly alert both the affected individuals and the Data Protection Board of India, and to follow a staged reporting approach to the regulator.

OPERATIONAL DESIGN FOR INDIVIDUAL NOTIFICATIONS

In practice, organisations will need pre-approved templates, language guidelines, and a clear internal escalation path so that notifications to individuals can be issued rapidly without waiting for lengthy legal or management approvals. For many businesses, this will also require defining “critical” sectors or user segments where more direct channels (for example, outbound calls or priority alerts) are triggered automatically for certain categories of breaches.

COORDINATING WITH THE DATA PROTECTION BOARD

The staged reporting model means that legal, security, and compliance teams must be able to assemble a preliminary picture of the incident very quickly, and then refine it into a structured 72-hour report. Internal incident playbooks should therefore distinguish between facts that are needed for the first intimation and those that require deeper forensic analysis, while ensuring that an audit trail is maintained for any corrections or clarifications provided to the Board.

IMPACT OF THE NO HARM THRESHOLD

Because the Rules do not allow organisations to screen out “low-risk” incidents, even relatively contained or short-lived breaches involving personal data fall within the reporting net.

This shifts the focus from subjective harm assessments to robust detection, classification, and documentation of every instance of unauthorised access or leakage. Organisations will need to tune their incident response processes, logging, and training so that smaller events are captured and escalated, rather than being informally resolved and forgotten.

ILLUSTRATIVE SCENARIO

- **Digital Lender Data Leak:** Imagine a digital lender suffering a cyber incident where hackers accessed customer loan files. Under Rule 7, the digital lender shall immediately draft a notice to all impacted borrowers (perhaps via email and SMS).
- **The notice might say:** *"We regret to inform you that on [Date], our systems experienced a data breach. Some of your personal loan application details (name, contact, and loan account information) may have been exposed. We are taking steps to secure our servers and have reset your account credentials as a precaution. Please be alert to any suspicious communications. We have reported this incident to the authorities. You can contact our helpdesk for further information."*
- At the same time, the digital lender would send an initial breach intimation to the Data Protection Board with what is known so far. Within 72 hours, the digital lender's team shall investigate and file a comprehensive report to the Board, detailing how the breach occurred (e.g. a specific server vulnerability), how many customers were affected, what steps were taken to plug the leak and assist customers, and plans for system upgrades or audits to prevent a repeat.
- **In a health-tech scenario, the requirements are analogous:** if a healthcare startup discovers a leak of patient records, it shall promptly inform all patients (e.g. via email/SMS and perhaps a public notice on its app) and report to the Board.
- Even if only a small number of patient files were exposed, the obligation to notify remains, reflecting the high sensitivity of any personal medical data. The swift, transparent communication not only keeps users informed but also demonstrates the organization's accountability in handling the crisis.

Ensure compliance with BCP protocols & verify encryption, access control, audit trails, VPRA of vendors.

Check if DSA/DMA contracts prohibit data use beyond purpose & confirm clause-wise alignment with DPDP and DL Directions.

Review incident log and simulation reports & confirm 72-hour reporting capacity and CERT-In/RBI escalation workflow.

Confirm disclosures in loan documents per DL Directions & ensure training and monitoring mechanisms on data handling.

Data of Children and Persons with Disabilities

The DPDP Rules require Data Fiduciaries to obtain and verify consent from a parent or lawful guardian before processing the personal data of children (under 18 years) and certain persons with disabilities, going beyond simple checkboxes or self-declarations.

Detect child / Disability: Use date of birth or disability indicators to flag users needing guardian consent.

Pause Processing: Hold personal data processing until verified guardian consent is obtained.

Start Consent Workflow: Redirect to a parent/guardian consent flow (email, link, or on-screen flow).

Verify Consent: Use at least one approved method to confirm the adult's identity and authority.

Process for specific purposes only: Process the child's or represented person's data only for the purposes approved by the guardian.

Use an already authenticated parent or guardian account. Example: adding a child profile under a verified parent telecom or platform account. Parent's verified identity serves as the basis for consent on the child's behalf.

Ask the person claiming to be the parent/guardian to provide proof of identity and age. Example: upload a government-issued ID or enter an ID number for verification. Where needed, request proof of relationship (for example, in high-risk contexts such as health or education data).

Use a digital token or credential issued by an authorised authority. Example: integrating with a government-approved age/guardian-verification or DigiLocker-style service. Token confirms that the consenting adult is over 18 and is the parent or lawful guardian tied to the child.

OPERATIONAL IMPLICATIONS FOR PRODUCT AND COMPLIANCE TEAMS

User journey design: Product teams should configure sign-up and profile-edit flows so that date of birth and disability-related flags are captured early and evaluated in real time. Where a user is identified as a child or as someone whose data can only be processed through a guardian, the system should automatically block further steps and present the guardian consent flow, rather than silently accepting the user's own click on "I Agree".

Handling verification artefacts: Compliance and privacy functions will need a clear position on how long to retain copies or tokens of parental/guardian verification, and how to secure them. Collecting government IDs or tokens introduces its own data-protection risks, so organisations should apply data minimisation, strict access controls, and, where possible, rely on one-time verification tokens instead of permanently storing full documents.

Managing new purposes over time: Over the lifecycle of a service, new features, analytics uses, or partnerships may create fresh purposes for processing children's or represented persons' data. Each such change should trigger a check in the consent records and, where necessary, a new guardian consent request tied to the additional purpose. Internal change-management processes should therefore treat "new data purposes" as an event that automatically requires a guardian consent impact review.

EXAMPLE – EDTECH & DIGITAL WALLETS

Consider a learning app aimed at teenagers. When a 16-year-old tries to register, the app should not just let them complete signup solo. Instead, it might require a parent's email or phone number. The parent would then receive a link to provide consent. The app could ask the parent to log in with their own verified account or submit an ID for age verification. Only after the parent's identity is verified and they explicitly consent (e.g. by ticking checkboxes for different data uses like profile creation, progress tracking, etc.), will the teen's account become active. Similarly, a digital wallet offering accounts for 17-year-olds would build a step where a guardian's authenticated approval is mandatory. For instance, the minor fills in their details, then the wallet app sends an OTP or confirmation request to the parent's registered mobile number, which the parent shall approve and perhaps verify their PAN/Aadhaar for age proof. This ensures the consent on record is truly from an adult guardian, not the child pretending.

EXEMPTIONS FOR ESSENTIAL SERVICES (CHILDREN)

WHAT IS ALLOWED WITHOUT PRIOR CONSENT?

Healthcare providers can treat a child and access records in emergencies.

Schools can monitor or track students on campus for safety and educational purposes.

Daycare and similar services can act for health, safety, and welfare within their mandate.

Government welfare schemes can process children's data to deliver benefits

WHO GETS THE EXEMPTION

Trusted providers of essential services for children.

Examples: hospitals, clinics, schools, daycare centers, welfare agencies.

Listed in the Fourth Schedule for specified activities.

LIMITS OF THE EXEMPTION

Exemptions are tightly defined and linked to specific entities and purposes.

They cover activities like health services, safety, education, and welfare programmes.

Outside these defined cases, the default rule is strict, verifiable parental consent.

PERSONS WITH DISABILITIES – GUARDIAN CONSENT

A person with legal authority under Indian law to act for the individual. May be appointed by a court under guardianship laws. May be authorised under the Rights of Persons with Disabilities Act, 2016. May be recognised under the National Trust Act, 1999 or other competent authority.	Certain persons with severe physical or intellectual disabilities. Individuals who cannot provide informed consent even with support. Situations where someone else must act on their behalf for data decisions	Service captures guardian's details and supporting documents. Requires proof of guardian status. Consent or instructions are accepted only after verification. Guardian's consent stands in place of the Data Principal's, but only within the legal scope of that guardianship.

Common principle: Exemptions for essential services are narrow, and guardian consent must be verifiable. Outside these specific situations, organisations shall obtain and confirm parental or lawful guardian consent before processing personal data of children or covered persons with disabilities.

PRACTICAL IMPLICATIONS FOR SERVICE DESIGN AND COMPLIANCE

Building guardian flows for disability cases: Where services target or are likely to be used by persons with significant disabilities, onboarding flows should explicitly ask whether the user is acting as a lawful guardian and, if so, prompt for the relevant legal documentation. Simply allowing a caretaker to tick a box saying "I am the guardian" is not sufficient; systems must be able to receive, validate, and securely store or record proof of guardianship in a way that can be audited later.

Scope and review of guardian authority: Once a guardian is verified, product and legal teams should ensure that the guardian's consent is only relied upon within the scope of the underlying legal authority. If the court order or statutory appointment limits decisions to certain domains (for example, medical decisions only), the service should not treat that consent as a blanket authorisation for all processing. Over time, there should also be mechanisms to update or re-verify guardian status if the underlying legal appointment changes or expires.

EXAMPLE – HEALTHCARE SCENARIO

- A telemedicine platform for mental health may have users who are adults under guardianship due to severe mental conditions.
- Under the new rules, if a caregiver is setting up the patient's profile and giving consent for treatment data to be processed, the platform should verify that this caregiver is the patient's lawful guardian (e.g. through a government-issued guardian ID or court letter).
- If the caregiver cannot prove legal guardianship, the platform cannot rely on their consent for data processing.
- In such cases, the platform might need to deny services or find an alternative legal basis until proper consent is obtained.
- On the other hand, if an unconscious or incapacitated patient is brought to a hospital, doctors can still proceed with life-saving treatment and handle the data under emergency exceptions (they don't have to wait for a guardian consent in an emergency).
- But for routine matters and digital services, compliance teams should build in checks for guardian authorization whenever someone other than the data principal is granting consent on the latter's behalf.

Significant Data Fiduciary (SDF)

It is an organisation whose scale or sensitivity of data processing triggers additional duties such as annual Data Protection Impact Assessment (DPIAs), independent audits, algorithmic accountability, stronger governance, and possible data transfer restrictions, once formally designated by the government or the Data Protection Board.

WHO CAN BE A SIGNIFICANT DATA FIDUCIARY?

Formally designated by the government or the Data Protection Board.

Criteria under the DPDP Act

Volume of personal data processed; Sensitivity of data (for example, health or biometric data); Number of users and geographic reach; Risk to rights and potential societal impact; Turnover and economic significance.

Likely Candidates

Big tech platforms (social media, large e-commerce); Major banks, NBFCs, and large fintechs; Large telecom and IT service providers; Health-tech platforms and critical ID or payments infrastructure.

ANNUAL DPIA

At least once every 12 months; Systematic review of how processing (including new projects/tech) affects privacy; Identify harms (breaches, profiling, biases) and mitigation measures; Example: assessing an AI recommendation feature for sensitive profiling risks

ANNUAL INDEPENDENT DATA AUDIT

Periodic audit by an independent evaluator; Reviews compliance with the DPDP Act and Rules, security, and governance; SDF submits DPIA and audit reports or summaries to the Data Protection Board; Enables regulators to spot red flags and monitor continuous accountability.

ALGORITHMIC ACCOUNTABILITY

Check that automated systems and algorithms do not harm Data Principals' rights; Assess for bias, discrimination, privacy intrusion, and opaque decision-making; Document "algorithmic impact assessments" for AI, profiling, and scoring models; Be ready to demonstrate to regulators that key systems are rights-compliant.

DATA PROTECTION OFFICER AND GOVERNANCE

Appoint a Data Protection Officer as a clear, identifiable contact point; DPO oversees compliance and reports to senior management; Publish DPO contact details; Elevate privacy to board/senior-management level; Treat privacy risk alongside financial and operational risks, given penalties up to INR 250 Crore.

COMPLIANCE WITH DATA TRANSFER RESTRICTIONS

Government may direct that certain categories of SDF-handled data not leave India.

A form of targeted data localisation for sensitive or critical data types.

SDF must adapt architecture (for eg, local servers, data segregation) to comply.

Must monitor regulatory notifications closely and adjust cross-border data flows.

WHAT SHOULD POTENTIAL SDFS DO NOW?

Identify if your scale, data sensitivity, and user base make SDF designation likely

Start conducting regular DPIAs and trial independent audits even before formal designation

Map key algorithms and profiling systems and introduce bias/impact testing

Put a DPO and privacy governance structure in place early

Build flexibility into data infrastructure to respond to localisation directions

PRACTICAL IMPLICATIONS AND READINESS FOR SDF DESIGNATION

Integrating DPIAs into product lifecycle: For organisations that are likely SDF candidates, DPIAs should not be treated as an annual paperwork exercise but built into the product and change-management lifecycle.

Any major new feature, data integration, or technology stack change should trigger a DPIA checkpoint so that privacy risks are analysed before launch rather than retrospectively. This is particularly important where new models, cross-product data sharing, or third-party integrations are introduced.

Using audits as a governance tool: Independent data audits can provide boards and senior executives with a structured view of weaknesses in controls, policies, and culture. Rather than approaching audits purely as a compliance cost, SDFs can use them to benchmark themselves against peers, justify investments in security and privacy tooling, and demonstrate to regulators and customers that issues are being identified and addressed in a disciplined way.

Managing algorithmic risk at scale: Where an organisation relies heavily on automated decision-making, small design choices in models or data sets can have large downstream effects on groups of users. SDFs should therefore maintain an inventory of high-impact models, define what counts as “adverse effect” for their context, and ensure there is a repeatable process for testing, documenting, and remediating algorithmic risks.

Over time, this can evolve into a formal “algorithmic governance” programme that ties together model documentation, fairness checks, explainability tools, and escalation routes when users challenge automated outcomes.

Preparing for closer regulatory engagement: Once designated, SDFs can expect more frequent and detailed engagement from the Data Protection Board, including queries about DPIA conclusions, audit findings, and mitigation steps. Mature SDFs will anticipate this by tightening their documentation, clarifying lines of responsibility for responding to regulatory requests, and conducting internal “mock inquiries” or tabletop exercises to test how quickly and clearly they can explain their data protection posture.

Reasonable Security Safeguards

Rule 6 of the DPDP Rules turns security from a generic IT best practice into an explicit legal obligation. Data Fiduciaries must implement “reasonable security safeguards” across technology, processes, and vendors to prevent unauthorised access, use, alteration, or loss of personal data.

DATA ENCRYPTION AND MASKING

Encrypt personal data at rest and in transit (e.g. databases, APIs, web traffic); Use hashing, tokenisation, or masking for sensitive fields (e.g. show only last 4 digits); Limit internal exposure so that even if systems are accessed unlawfully, data is not visible in plain text.

ACCESS CONTROL AND AUTHENTICATION

Grant access to personal data only to authorised users and systems; Use strong authentication (unique IDs, strong passwords, multi-factor where appropriate); Apply role-based access so staff only see what they need for their role; Promptly revoke access when staff leave or change roles.

ACTIVITY LOGGING AND AUDIT TRAILS

Log who accessed which records, when, and what action they took; Capture key events such as view, edit, export, and deletion of personal data; Protect logs from tampering and review them regularly; Retain logs for at least one year for investigation and audit purposes.

CONTINUOUS MONITORING AND INCIDENT DETECTION

Monitor systems and logs on an ongoing basis for suspicious activity; Use tools such as intrusion detection, anomaly detection, and alerting; Conduct regular vulnerability scans and penetration tests; Treat security as an ongoing process of assessment and improvement, not a one-time setup.

ORGANISATIONAL & ECOSYSTEM SAFEGUARDS

ONE-YEAR MINIMUM RETENTION FOR SECURITY

Keep relevant data and logs for at least one year for security and investigation; Do not immediately erase all traces when a user closes an account or a service ends; Ensure archived records are securely stored and access-controlled.

BUSINESS CONTINUITY AND DATA RECOVERY

Maintain encrypted backups of personal data and critical systems; Plan for incidents such as server failures, ransomware, or disasters; Test that data can be restored in a timely manner; Ensure services to Data Principals can resume even after major disruptions.

SECURE OUTSOURCING AND VENDOR CONTRACTS

Flow down security requirements to processors and third-party vendors; Include contractual clauses on confidentiality, security controls, and breach notification; Ensure outsourced services meet equivalent security standards; Review and update Data Processing Agreements to align with DPDP expectations.

ORGANISATIONAL MEASURES AND SECURITY CULTURE

Conduct background checks for staff handling sensitive data where appropriate; Train employees on data security, phishing, and incident reporting; Restrict use of portable media and enforce clear data-handling policies; Maintain documented procedures such as an incident response plan and security guidelines.

PRACTICAL IMPLEMENTATION AND GOVERNANCE CONSIDERATIONS

Risk-based definition of "reasonable": Although Rule 6 sets out minimum expectations, what counts as "reasonable" will still depend on the nature of the business, the sensitivity and volume of data, and the threat landscape. Larger or higher-risk Data Fiduciaries should expect regulators to look for more mature controls, such as formal risk assessments, security certifications, and layered defences. Smaller entities handling less risky data may implement simpler controls, but they still need to be able to explain how their safeguards are proportionate to the risks they face.

Aligning security, privacy, and retention: The one-year retention requirement for logs and security-relevant data can appear to conflict with "data minimisation". Organisations will need to explicitly separate "business" retention periods from "security" retention periods in their policies, documenting why certain data and logs are retained longer purely for investigation and accountability. It is important that these retained copies are clearly tagged, access-restricted, and, where feasible, pseudonymized to reduce residual risk.

Making vendors part of the control environment: Many breaches originate at third-party service providers rather than at the Data Fiduciary itself. A mature approach to Rule 6 involves treating vendors as extensions of the internal control environment: performing due diligence before onboarding, periodically reviewing their security posture, and having a structured process for evaluating their incident reports. Legal, procurement, and security teams should work together so that commercial contracts, technical controls, and operational practices are aligned rather than handled in isolation.

From policy document to day-to-day behaviour: Finally, security safeguards only have real value if they influence everyday behaviour. This means translating Rule 6 into clear internal do's and don'ts, incorporating security checks into normal workflows (for example, access requests, change management, software releases), and ensuring there is visible support from senior management when security controls cause friction. Regular drills, simulated phishing campaigns, and post-incident reviews help reinforce that security is a shared responsibility rather than a purely technical concern.

Conclusion

The DPDP Act, 2023 and DPDP Rules, 2025 collectively mark a shift from informal, IT-led privacy practices to a formal, legally enforceable data protection regime with clear accountability for senior management and boards.

Compliance is not a one-time documentation exercise but an ongoing governance function that must be embedded into product design, vendor management, security operations, and incident response.

Organisations that approach the framework as a “checklist” are likely to struggle, especially once breach-notification, DPIA, and audit obligations begin to be tested in practice.

A pragmatic way forward is to prioritise:

(a) mapping data flows and rationalising data retention;

(b) redesigning consent and notice mechanisms;

(c) uplifting technical and organisational security safeguards;

(d) instituting breach management, logging, and business continuity arrangements; and

(e) creating clear ownership at the board and senior-management level for privacy risk.

If implemented thoughtfully, the DPDP framework can become an enabler for trusted digital business models, cross-border data use, and responsible innovation, rather than merely a constraint or cost centre.

Contact us

Ground Floor, H No. 27-A, Hauz Khas Village,
New Delhi, 110016
Office: +91 11 41727676
info@akandpartners.in
www.akandpartners.in