Deloitte.

# India's DPDP Rules 2025
# Leading digital privacy compliance

**November 2025**

# Table of contents

# Introduction

India marked a pivotal moment in its privacy regulation landscape in November 2025 with the Ministry of Electronics and Information Technology (MeitY) issuing the notification for the enforcement of the Digital Personal Data Protection Act, 2023 (DPDPA), and the Digital Personal Data Protection Rules, 2025 (Rules).

The Rules, notified in November 2025, establish a pathway for organisations to manage personal data while enhancing Data Principals' control over their personal data.[1] The question now is what this means for companies already working towards compliance. While certain stakeholders may argue that the framework could benefit from additional clarity, particularly regarding definitions and operational thresholds, the core strength lies in its phased, pragmatic rollout. Businesses that have proactively embedded privacy into their processes will only need targeted refinements to meet the new standards. While the DPDP rules are meant for organisations to get themselves compliant with the DPDP Act, they also provide a model for global organisations that have started on this journey. These organisations can use their existing global frameworks and plug in the DPDP-specific requirements into their ecosystem.

## Key coverage

These Rules outline the obligations of a Data Fiduciary in a manner that goes beyond the typical provisions found in other data protection regulations. From this perspective, the following key aspects will be discussed.

- Our perspective and interpretation of the Rules through a practical, business-and operations-centric lens.
- The actionable compliance journey towards data protection readiness and the areas where companies must make additional efforts to comply with these Rules.
- FAQs: Our approach towards the compliance challenges that businesses usually come across.

[1] https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf

# From draft to final: Key developments in DPDP Rules

The journey from the Draft DPDPA Rules (Draft Rules) released in January 2025 to the finalised Rules notified in November 2025 reflects a regulatory framework that has matured meaningfully, moving from a largely prescriptive draft to a more calibrated, operationally grounded and implementation-sensitive regime. The most defining shift between the two versions is in the text of individual Rules and in the regulatory philosophy that emerges when the final Rules are read holistically.

### A more realistic and phased compliance architecture

One of the most significant departures from the Draft Rules is the introduction of a clear, phased compliance schedule. The Draft Rules, while comprehensive, placed almost immediate compliance expectations on organisations without acknowledging the investment, restructuring and systems-level changes required to operationalise many of the obligations. The final Rules sensibly stagger compliance. The foundational provisions and the Data Protection Board (DPB) framework take effect immediately, while the Consent Manager requirements will come into force after a year, and the core operational compliance obligations are deferred to an 18-month window. This phased structure signals a regulator that recognises the compliance realities on the ground, regardless of their global or local stature. It gives organisations time, not to delay compliance, but to build it meaningfully, sustainably and with the necessary internal alignment.

### Sharper drafting and clearer segmentation of obligations

The evolution from Draft Rules to final Rules has also improved clarity in several areas. The separation of Rules governing children's data from those governing the personal data of persons with disabilities is particularly noteworthy. In the Draft Rules, these were bundled together, creating interpretational ambiguities about how fiduciaries should differentiate between consent mechanisms and risk thresholds.

In the final Rules, each of these categories is carved out into its own dedicated provision. This is more than a drafting improvement. It helps organisations implement these Rules without reliance on broad assumptions or internal reinterpretation.

### A material shift in data retention obligations

Perhaps the most profound change is the broad expansion of the one-year data retention requirement. The Draft Rules imposed retention expectations largely for logs and specific categories of processing data. These Rules go significantly further, requiring fiduciaries to retain personal data, traffic data and logs generated during processing for a minimum of one year.

From a compliance and risk management perspective, this change will be felt across every sector. Organisations will need stronger logging frameworks, more scalable storage infrastructure and hardened security practices to mitigate the risk that comes with storing larger volumes of data for longer periods.

While the intent is to have enforcement transparency, better investigation support and audit readiness, the operational responsibilities pertaining to this requirement need to be considered by Data Fiduciaries and Data Processors as applicable. Organisations may need to revisit and redesign their data lifecycle strategies to reconcile retention obligations with deletion requirements.

### Consent Managers and accountability remain strongly emphasized

While the final Rules defer the effective date for Consent Manager obligations, the underlying accountability expectations remain largely unchanged. Consent Managers, once operational, will play a critical role in India's data protection ecosystem by offering a consent-layer that is interoperable, transparent and standardised across service providers.

This delay should not be interpreted as dilution. Instead, it gives fiduciaries and start-ups sufficient time to develop consent-layer technology and align their operational, financial and technical capabilities to regulatory expectations.

When viewed together, the final DPDPA Rules reflect a shift towards regulatory pragmatism without compromising on user protection. Compared with the Draft Rules, the final framework is more structured, more precise and more responsive to the operational realities that organisations face.

# What these Rules mean for you

These Rules clearly delineate the applicability of their provisions, specifying that certain obligations are enforceable immediately from the date of notification, while others are subject to phased enforcement within defined timelines of 12 and 18 months. This structured approach provides organisations with clarity on immediate compliance requirements and allows a defined period to operationalise obligations that require longer-term implementation.

## Rules applicable from 13 November 2026

### 1. Consent managers and digital locker service providers

- DPDPA introduces the concept of data portability, facilitated by Consent Managers, which is envisioned to function similarly to Unified Payments Interface (UPI) platforms. These Consent Managers, operating as applications or websites, will enable Data Principals to seamlessly share their personal data with multiple Data Fiduciaries. Acting as centralised and user-friendly intermediaries, they will provide Data Principals control over their data. However, certain caveats are imposed. Similar to the Reserve Bank of India's (RBI) Account Aggregator framework, Consent Managers must register with the Data Protection Board of India (DPBI). To qualify, they must meet specific conditions outlined in the Rules, including demonstrating adequate technical, operational and financial capacity.
- Consent Managers are tasked with maintaining comprehensive records of consent transactions, encompassing approvals, denials and revocations of requests initiated by Data Fiduciaries. Furthermore, they must support Data Principals by providing these records in a machine-readable format, ensuring transparency and facilitating efficient data management.

## Rules applicable from 13 May 2027

### 1. Consent and notice

- It would be highly beneficial to draft the notice in 22 Indian languages, ensuring inclusivity and accessibility for a diverse range of Data Principals. Additionally, presenting the notice in an audio-visual format can enhance user engagement and understanding, providing an interactive way for Data Principals to receive support. This approach would accommodate each sector, ensuring communication is clear and accessible regardless of linguistic or technological barriers.
- The Data Protection Officer's (DPO) office should regularly review and update the notice to reflect changes in product, service or personal data requirements. This ensures alignment with evolving operational needs and legal compliance. Any updates to the notice should be promptly communicated to Data Principals, ensuring transparency and maintaining trust.
- Clear and precise communication about the purpose and necessity of collecting personal data is crucial, ensuring that it aligns with the specific products or services offered. Each data point should be explicitly mapped to its intended use to enhance transparency and understanding. Structured, layered explanations supported by real-world examples and accessible formats such as FAQs or tooltips can further ensure clarity and foster trust with Data Principals.
- The notice should include a direct link to a section for easily managing and withdrawing consent, with alternative methods such as email or a toll-free number for accessibility. Withdrawal should be as simple as granting consent, ideally with a one-click option. An automated acknowledgement should confirm the action. This ensures compliance and transparency and builds trust through clear, user-friendly options for managing consent. The notice should provide clear, direct instructions and accessible links for Data Principals to easily exercise their rights under the DPDPA or file complaints with the DPB. This ensures a simple and straightforward process through multiple channels such as the website, email or phone.

### 2. Consent from children and persons with disabilities

- The Data Fiduciary must prioritise the child's well-being by ensuring that products and services are designed with Privacy-by-Design (PbD) principles. This approach ensures that only the minimal amount of data necessary for the child's usage is processed, aligning with best practices for data privacy while optimising the product's functionality for the child. There is zero tolerance for tracking children by location, behavioural monitoring and targeting advertising at them. This highlights a need for additional security measures to provide reliable privacy assurance to customers to gain their trust.
- Under the Guardians and Wards Act, 1890, the person who

claims to be a parent or lawful guardian should do so by providing the necessary details on the mobile application/ website/any other alternative method provided by the Data Fiduciary to be eligible to provide consent on behalf of the children. It is important to consider the religion-based guardianship provisions outlined in various laws, relating to the relevant applicable local laws and regulations.

- To determine the scope of a person with a disability, one must submit appropriate documents of guardianship as mandated by the applicable local laws and regulations to be eligible to provide consent on behalf of the person with a disability.
- The Data Fiduciary must implement effective verification mechanisms for parental consent so that the Data Fiduciary can reference reliable identity and age details already available within their system or obtain with the prior consent of the individual, ensuring the information is accurate and up to date.
- A potential method for achieving this could involve the Data Fiduciary using an electronic token linked to an individual's identity and age. This token should be generated by a trusted entity, such as a government-authorised entity or a digital locker service provider. It should be generated in accordance with legal provisions and the terms governing the entity's authorisation, ensuring consistency with legal requirements.
- Maintaining user accounts is an additional obligation for the Data Fiduciary to monitor updates in the profiles of children and persons with disabilities. Profiling should be avoided to promote any other processes to comply with Section 9 of the DPDPA, 2023.

**3. Reasonable security safeguards**

- These Rules reflect the importance of robust data protection measures to be followed by organisations. The existing organisational and technical measures should be assessed to understand the gaps and protect the personal data management landscape.
- Implementing encryption and techniques such as obfuscation or masking represent an industry-standard approach to safeguarding privacy, aligning with the principles across the global privacy regulations such as those in General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Personal Information Protection and Electronic Documents Act (PIPEDA) and Personal Data Protection Act (PDPA), which advocate for encryption and pseudonymisation as key methods in data protection. The implementation must ensure that encryption protocols are up-to-date and strong enough to protect against evolving cyber and privacy threats.
- Reasonable security safeguards with mandatory baseline requirements offer organisations the flexibility to implement controls such as encryption and access management based on their risk profile without prescribing specific standards if the baseline criteria are met.
- These Rules mandate robust control and visibility over access to personal data, along with early detection of unauthorised activities. This can be accomplished through measures such as Single Sign-On (SSO), Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), periodic access reviews, privileged users activity logging and monitoring, enforcing strong password policy, securing credentials of privileged users, secrets management and integration of malicious access alerts with central security operations and monitoring teams. These safeguards ensure that only authorised individuals can access personal data, and can be implemented by using a centralised identity and access governance platform.
- With the growing prevalence of remote work and cloud-based environments, it is essential to implement, govern and monitor security protections for endpoints and cloud services. This includes deploying endpoint security solutions, Cloud Access Security Brokers (CASB) or equivalent technologies, alongside vulnerability management and patch management processes.
- Safeguards such as, but not limited to, data integrity checks (such as checksum/hash functions), logging and monitoring measures, backup and restoration mechanisms shall be applied to ensure the confidentiality, integrity and availability of personal information is maintained.
- The Data Fiduciary's DPO team/equivalent authority, as applicable, should notify the legal team in a timely manner about the latest amendments regarding reasonable security safeguards for contracts with Data Processors and Data Fiduciaries. A standard clause incorporating these safeguards should be added to all contracts in line with the Rules.

**4. Personal data breach notification**

- The DPDPA and Rules place significant emphasis on timely detection, reporting and management of personal data breaches to protect the rights and interests of Data Principals. Organisations are required to implement robust incident response mechanisms to identify, assess, contain and remediate breaches effectively. A personal data breach may include unauthorised access, disclosure, alteration, loss or destruction of personal data, whether accidental or deliberate.
- Organisations must maintain detailed audit logs and records of all incidents, documenting the type of breach, categories of data affected, impact on individuals, root cause analysis, mitigation measures and timelines of detection and resolution. These logs should be readily available for review by the DPB and internal audit teams, ensuring accountability and regulatory compliance.
- Notification obligations are critical under these Rules. Organisations must report personal data breaches to the DPB within the prescribed timelines, providing a clear and accurate account of the breach, its impact and the remedial actions undertaken. Additionally, affected Data Principals

must be informed within the prescribed timelines when the breach is likely to result in significant harm, loss or risk to their rights. Notification should be concise, transparent and actionable, outlining the nature of the breach, potential consequences and recommended steps for mitigating any risks.

- The Data Protection Officer (DPO) or designated breach response team should regularly review and update incident response policies to reflect operational changes, emerging threats or regulatory updates. Automated systems for logging incidents, sending notifications and tracking remedial actions can significantly improve responsiveness, ensure audit readiness and demonstrate accountability.

**5. Data retention**

- This provision is significant as it emphasizes the principle of data minimisation, ensuring that personal data is not retained for longer than necessary. Data Fiduciaries would have to provide a clear justification for any personal data retained beyond the specified period.
- There are currently no clear guidelines regarding the format of communication for data erasure or the channels that should be used for this communication. It would benefit the Data Fiduciaries to use multiple channels to ensure the Data Principal receives the communication.
- These Rules have considered three major Data Fiduciary classes: social media, e-commerce and online gaming. Additionally, data fiduciaries may also include utility websites, banking and fintech platforms, quick commerce, big tech platforms and telecom websites. Specifying data retention periods offers a vast range of possibilities, serving as insightful guidance and a baseline for data fiduciaries to align their practices.
- The requirement to retain personal data, associated traffic data and processing logs for a minimum period of one year introduces a baseline compliance obligation that applies uniformly across all Data Fiduciaries. This ensures that organisations maintain adequate records to support investigations, audits and regulatory inquiries. However, this minimum-period mandate also necessitates the establishment of structured log-management practices covering storage, security, access control and erasure. Data Fiduciaries must clearly define systems to automate the one-year retention cycle while ensuring that any extension of retention is grounded in a legitimate legal requirement, supported by documented justification and executed without undermining the principle of data minimisation.
- Organisations need to adhere to secure disposal, archival and storage requirements of personal data in line with the industry best practices. Data Fiduciaries would have to establish secure disposal procedures (such as encryption, wiping or physical destruction of data) for when data is no longer needed.

**6. Significant Data Fiduciary (SDF)**

- Significant Data Fiduciaries (SDF) under the DPDPA have additional obligations, such as but not limited to institutionalising an enhanced governance framework anchored in accountability, transparency and consistent oversight. A DPO based in India must be appointed as the primary point of contact for regulatory interactions and operational compliance. In addition, SDFs are required to conduct annual independent audits to assess the effectiveness of their privacy controls and ensure alignment with the DPDPA and Rules. A Data Protection Impact Assessment (DPIA) must be undertaken for all processing operations involving high risk, particularly where profiling, automated decision-making or large-scale processing is involved. These assessments must be formally documented and made available for scrutiny by the DPB when required.
- To support this enhanced governance posture, SDFs must maintain robust logging and continuous monitoring mechanisms, allowing audit trails to be generated for all data processing activities, security events and system interactions. Organisations must also retain detailed records for longer periods where risk necessitates enhanced visibility. Where AI and agentic-AI systems are deployed, SDFs must demonstrate algorithmic transparency by documenting logic, potential biases, safeguards and user impact, ensuring regulatory authorities can examine systems for fairness, accuracy and compliance. Overall, the SDF framework places significant emphasis on proactive governance, requiring organisations to embed privacy considerations into organisational decision-making, operational processes and risk management structures.

**7. Data Principal rights**

- Organisations must implement structured, user-friendly mechanisms that allow Data Principals to easily exercise rights such as access, correction, updating, erasure, grievance redressal and nomination. These mechanisms should be easily accessible, multilayered and available through multiple channels, such as digital dashboards, mobile applications, email support and toll-free helplines. A key expectation under these Rules is the establishment of an authentication mechanism that is secure yet user-centric, ensuring that rights requests are fulfilled only after verifying the identity of the requester without creating undue friction.
- Once a request is submitted, organisations are required to process it per industry best practice timelines, while adhering to grievance redressal timelines mentioned in the Rules.
- The request shall be processed in a transparent manner, maintaining accountability through clear communication and status updates. They must also keep detailed records of each rights request, including acknowledgements, decisions

taken and timelines for closure. For requests such as erasure, organisations must ensure alignment with other statutory obligations, particularly retention requirements, while still respecting the individual's right to deletion wherever applicable. The right to nomination, enabling a Data Principal to appoint another individual to exercise rights in the event of incapacity or death, introduces an added dimension of user autonomy and futureproofing.
By operationalising these rights, organisations reinforce trust, demonstrate respect for user autonomy and uphold the fundamental principles of fair and transparent processing.

**8. Transfer of personal data outside India**

- Rules outline that personal data processed by a Data Fiduciary cannot be transferred to a foreign country unless certain requirements prescribed by the central government are met. The Data Fiduciary must comply with government-mandated requirements regarding transfer of such data to foreign states or entities/agencies under their control.

## Implementation timeline for the Act and Rules:

Digital Personal Data Protection Act and Rules will follow a phased implementation schedule as noted below:

| Timeline | Act | Rules |
|---|---|---|
| 13 November 2025 (Applicable from the date of publication) | **Section 1(2) -** Short title and commencement | **Rule 1–** Short title and commencement |
| | **Section 2 -** Definitions and Interpretation | **Rule 2 –** Definitions |
| | **Section 18 –** Establishment of Data Protection Board of India (DPBI) | **Rule 17 –** Appointment of Chairperson and Members of DPBI |
| | **Section 19 –** Composition and qualifications for appointment of DPBI members | **Rule 18 -** Salary, allowances and terms and conditions of service of members of DPBI |
| | **Section 20 -** Salary, allowances payable to and term of office | **Rule 19 -** Procedure for meetings of DPBI |
| | **Section 21 –** Disqualifications for appointment and continuation as members of DPBI. | **Rule 20 -** Functioning of DPBI as a digital office |
| | **Section 22 –** Resignation by members and filling of vacancy | **Rule 21 -** Terms and conditions of appointment and service of employees of DPBI |
| | **Section 23 –** Proceedings of DPBI | |
| | **Section 24 -** Officers and employees of DPBI. | |
| | **Section 25** – Members and officers of public servants | |
| | **Section 26 –** Powers of Chairperson of DPBI | |
| | **Section 35, 38-43, 44(1) and 44(3) –** Procedural provisions and changes to current laws | |
| 12 November 2026 (Applicable for 12 months from the date of publication) | **Section 6(9) –** Registration with the DPBI | **Rule 4** – Registration of Consent Manager |
| | **Section 27(1)(d) -** Inquiry by Consent Manager, into potential data breach | |
| 12 May 2027 (Applicable from 18 months from the date of publication) | **Section 3 –** Application of Act | **Rule 3 -** Notice given by Data Fiduciary to Data Principal |
| | **Section 4 –** Grounds for processing personal data | **Rule 5 -** Processing of personal data for the provision or issue of subsidy, benefit, service, certificate, license or permit by the State and its instrumentalities |
| | **Section 5 –** Notice | **Rule 6 -** Reasonable security safeguards |
| | **Section 6 -** Free and specific consent | **Rule 7 -** Intimation of personal data breach |
| | **Section 7 –** Legitimate uses (processing without consent) | **Rule 8 -** Time period for specified purpose to be deemed as no longer being served |
| | **Section 8 -** General obligations of Data Fiduciary | **Rule 9 -** Contact information of the person to answer questions about processing |

| Timeline | Act | Rules |
|---|---|---|
| | **Section 9 –** Processing of personal data of children or persons with disability | **Rule 10 -** Verifiable consent for processing of personal data of a child |
| | **Section 10 -** Additional obligations of Significant Data Fiduciary | **Rule 11 -** Verifiable consent for processing of personal data of a person with disability who has a lawful guardian. |
| | **Section 11 -** Right to access Information about personal data | **Rule 12 -** Exemptions from certain obligations applicable to the processing of personal data of a child |
| | **Section 12 -** Right to correction and erasure of personal data | **Rule 13 -** Additional obligations of Significant Data Fiduciary |
| | **Section 13 -** Right of grievance redressal | **Rule 14 –** Rights of Data Principals |
| | **Section 14 –** Right to nominate | **Rule 15 -** Transfer of personal data outside the territory of India |
| | **Section 15 -** Duties of Data Principal | **Rule 16 -** Exemption from DPDP Act for research, archiving or statistical purposes |
| | **Section 16 –** Processing of personal data outside India | **Rule 22 -** Appeal to TDSAT (Appellate Tribunal) |
| | **Section 17 –** Certain exemptions | **Rule 23 -** Calling for information from Data Fiduciary or intermediary |
| | **Section 27 –** Powers and functions of DPBI | |
| | **Section 28 -** Procedure to be followed by DPBI | |
| | **Section 29, 30 –** Appeal to TDSAT (Appellate Tribunal) | |
| | **Section 31 –** Alternate dispute resolution | |
| | **Section 32 –** Voluntary undertaking | |
| | **Section 33, 34 –** Penalties for violation | |
| | **Section 36 -** Power to call for information | |
| | **Section 37 -** Power of Central Government to issue directions | |
| | **Section 44(2) –** Amendments to IT Act (Repeals existing SPDI Rules) | |

# Way forward: The compliance road ahead

The Digital Personal Data Protection Act (DPDPA), 2023, along with the Digital Personal Data Protection Rules, 2025, establishes a structured framework for all data fiduciaries in India. Organisations must now plan their compliance journey, aligning personal data processing practices with the law while considering their business-specific use cases.
The roadmap below outlines a phased approach for organisations that have not yet prioritised privacy compliance and for organisations that have already started their DPDPA compliance journey. The roadmap is categorised into quick/immediate takeaways, short-term takeaways and strategic/long-term initiatives, guiding organisations from initial alignment to sustained operational compliance.

### Phase 1: Quick wins – Immediate compliance activities (1–3 Months)

Objective: Achieve immediate alignment with DPDPA and Rules obligations and reduce exposure to regulatory risk.

***For companies already on the compliance journey:***

- Conduct an initial gap assessment to identify areas that can be addressed with quick wins.
- Validate existing data mapping, governance structures and the DPO appointment against Rules, ensuring roles and responsibilities are clearly documented.
- Update privacy policies, internal procedures and workflows to reflect the new obligations and timelines.
- Conduct awareness sessions for key stakeholders to reinforce DPDP requirements and escalation protocols for DPB inquiries.
- Review technical safeguards, including access controls, password policies and encryption, to confirm they meet DPDPA and Rules baseline expectations.

***For companies already on the compliance journey:***

- Conduct a comprehensive assessment of all personal data processing activities and determine applicability under the DPDPA and Rules.
- Appoint a DPO or authorised representative and communicate contact details across relevant interfaces.
- Map all data flows across business units and IT systems to understand exposure points.
- Implement foundational security controls to protect sensitive data and conduct introductory awareness sessions for key stakeholders, highlighting critical obligations under DPDPA and Rules.

*Advisory note: These actions are designed to achieve foundational compliance quickly, mitigating immediate regulatory exposure while preparing the organisation for deeper compliance initiatives.*

### Phase 2: Tactical wins – Intermediate compliance enhancements (3–12 months)

Objective: Build infrastructure and operational processes for sustained compliance.

***For companies already on the compliance journey***:

- Conduct a detailed gap analysis to align existing practices with the requirements laid out under the Rules.
- Integrate or enhance consent management systems to include all categories of personal data, including children's data and data of persons with disabilities.
- Update privacy notices and templates to ensure clarity, standalone accessibility and multilingual support where required.
- Strengthen technical safeguards, including encryption, masking, access control and audit logging.
- Validate breach notification workflows and ensure DPB reporting mechanisms are operational.

***For companies yet to start compliance:***

- Implement consent management systems from the ground up, consistent with DPDP specifications.
- Draft standalone, clear and comprehensive privacy notices, ensuring coverage for special categories of personal data.
- Establish data classification protocols to manage general, sensitive and children's data effectively.
- Deploy technical safeguards to secure all personal data and define breach response mechanisms.

*Advisory note: Tactical wins focus on process integration and operational readiness, allowing organisations to manage compliance effectively across functions and business units.*

### Phase 3: Strategic initiatives – Long-term compliance and governance (12–18 months)

Objective: Operationalise all DPDP obligations and integrate privacy governance into business processes.

***For companies already on the compliance journey:***

- Automate Data Principal rights management, including access, correction and erasure.
- Implement retention and deletion policies in accordance with timelines under the Rules.
- Conduct Data Protection Impact Assessments (DPIAs) either manually or through automated means.
- Implement PbD principles, establish governance frameworks in line with DPDPA requirements and global Privacy standards to ensure Data Fiduciary, Joint Data Fiduciary and Data Processor responsibilities are documented and maintained.
- Ensure robust technical safeguards, including encryption, masking/tokenisation and audit logs.
- Validate compliance with cross-border transfer Rules and establish parental/guardian consent mechanisms.
- Review and formalise contracts with processors and joint fiduciaries, embedding DPDP compliance obligations.
- Implement AI governance controls for algorithmic transparency, bias mitigation and explainability.

***For companies yet to start compliance:***

- Operationalise mandated processes, including privacy notices, rights enablement and breach reporting mechanisms.
- Establish DPIA procedures and a schedule for regular audits.
- Deploy robust security controls across all systems processing personal data.
- Implement lawful cross-border data transfer mechanisms and parental/guardian consent frameworks.
- Integrate AI governance measures to address automated decision-making obligations.
- Finalise agreements with processors and joint fiduciaries to ensure enforceable compliance clauses.

*Advisory note: Strategic initiatives aim to institutionalise compliance, creating an organisational framework capable of sustaining privacy governance, mitigating risk and demonstrating accountability to regulators and stakeholders.*

---

### Phase 4: Continuous compliance (Post 18 months)

Objective: Maintain, monitor and continuously enhance DPDP compliance.

***For companies already on the compliance journey:***

- Conduct periodic audits, DPIAs and compliance reviews to maintain alignment with evolving DPDP requirements.
- Monitor regulatory updates and adjust policies and procedures proactively.
- Maintain governance dashboards to track consent management, rights requests, breach incidents and overall compliance KPIs.
- Continue employee training and reinforce a privacy-focused organisational culture.
- Review security certifications and PbD frameworks periodically and ensure joint fiduciary arrangements remain compliant.

***For companies yet to start compliance:***

- Implement continuous monitoring tools for consent management, rights requests and data security adherence.
- Establish governance mechanisms to track compliance progress and mitigate risks proactively.
- Conduct ongoing awareness programmes to embed privacy into organisational culture.
- Maintain incident response plans, technical safeguards and privacy policies aligned with DPDP obligations.
- Schedule recurring audits to ensure long-term, sustainable compliance.

# FAQs

**Q1. What should be my organisation's first step in implementing DPDPA compliance?**
A: The first and most critical step is identifying whether the DPDPA applies to your organisation and mapping all personal data within your systems. This includes understanding where data is collected, stored, processed and shared. Once this visibility is established, you can undertake a structured gap assessment to understand what needs to be prioritised, such as consent practices, notice design, security safeguards or data retention. Without a complete data inventory, compliance efforts may remain inconsistent or incomplete.

**Q2. What are the requirements for notices to Data Principals?**
A: Notices provided to Data Principals must be clear, standalone and written in plain language. They should include an itemised list of the personal data being collected, explain the specific purposes for processing in relation to the goods or services offered, and provide direct links for withdrawing consent, exercising data rights and filing complaints with the DPB.

**Q3. What is a Consent Manager, and what is required for registration?**
A: A Consent Manager is an entity registered with the DPB under the Digital Personal Data Protection Act, 2023. It provides a secure, transparent and interoperable platform that allows individuals (Data Principals) to give, manage, review or withdraw consent for their personal data across multiple Data Fiduciaries. Under Rule 4, Consent Managers must be registered with the DPB and meet prescribed standards to enable safe consent discovery, withdrawal and management across all fiduciaries.

**Q4. What security safeguards must we implement to comply with the DPDPA?**
A: Organisations must adopt reasonable security safeguards, including encryption, access controls, identity management, vulnerability assessments, patching and continuous monitoring. The goal is to prevent unauthorised access and to detect and respond to threats in real time. Implementing Multi-Factor Authentication (MFA), Role-Based Access Controls (RBAC), logging privileged user activity and integrating access alerts with your cybersecurity team are essential practices.

**Q5. What are breach notification obligations?**
A: Fiduciaries must promptly notify affected individuals about any personal data breach and report the incident to the DPB within 72 hours. The report should include details of the breach and the remedial measures taken to address it.

**Q6. What are the Rules around data retention and deletion?**
A: Personal data and related logs must be kept for at least one year. For large platforms, data belonging to inactive users should be deleted after three years, and the platform must provide at least 48 hours' prior notice before deletion.

**Q7. In what language should our notices be drafted?**
The DPDPA encourages accessibility and inclusiveness. While English remains acceptable, best practice and increasingly necessary for diverse user bases is to provide the privacy notice in any language specified in the Eighth Schedule to the Constitution. Where possible, organisations should also offer audio or audio-visual versions to maximise accessibility, especially for individuals with limited literacy or digital abilities. Clear, multi-lingual notices are compliant, improve customer trust and reduce ambiguity.

**Q8. How is verifiable parental consent handled for children?**
A: Organisations must implement age verification and obtain verifiable parental consent for processing children's personal data. This should be done using trusted identity providers or secure methods such as Digital Locker Tokens.

**Q9. Why were separate Rules introduced for children and persons with disabilities?**
A: The Draft Rules combined these under one provision, but the final Rules split them into Rule 10 (children) and Rule 11 (persons with disabilities). This change ensures clarity because consent verification processes differ for minors and guardians, reducing ambiguity and enabling tailored compliance for vulnerable groups.

**Q10. What obligations apply to Significant Data Fiduciaries (SDFs)?**
A: Significant Data Fiduciaries have additional responsibilities, including conducting annual Data Protection Impact Assessments (DPIAs), undergoing independent audits and ensuring transparency in the algorithms they use.

**Q11. What are the cross-border data transfer requirements?**
A: Cross-border transfers of personal data are permitted but subject to restrictions specified by the Government of India (GoI). The government may, through a general or special order, prescribe requirements that shall be adhered to when transferring personal data outside the country. These requirements could relate to the transmission of personal data or its storage on cloud servers located in specific hosting zones, depending on the destination country. All other transfers of personal data must follow strict contractual safeguards and use authorised mechanisms to ensure the destination provides adequate protection. This approach ensures accuracy, safeguards confidentiality and upholds accountability while reducing the risk of insecure data flows. Further clarity on this topic is expected in the future.

**Q12. How does the appeals process work?**
A: If you disagree with a decision made by the DPB, there is a clear two-step appeals process. First, you can file an appeal digitally with the DPB for review. If you are still not satisfied with the outcome, you can escalate the matter to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT). TDSAT is required to resolve appeals within six months, ensuring a structured and time-bound process. These appeal routes apply to all DPB decisions, including those related to government data access requests.

# Connect with us

**Sathish Gopalaiah**
President, Technology & Transformation
Deloitte South Asia
sathishtg@deloitte.com

**Gaurav Shukla**
Partner and Leader – Cyber
Deloitte South Asia
shuklagaurav@deloitte.com

**Mayuran Palanisamy**
Partner
Deloitte India
mayuranp@deloitte.com

**Manish Sehgal**
Partner
Deloitte India
masehgal@deloitte.com

**Jignesh Oza**
Partner
Deloitte India
jigneshoza@deloitte.com

**Goldie Dhama**
Partner
Deloitte India
goldiedhama@deloitte.com

# Contributors

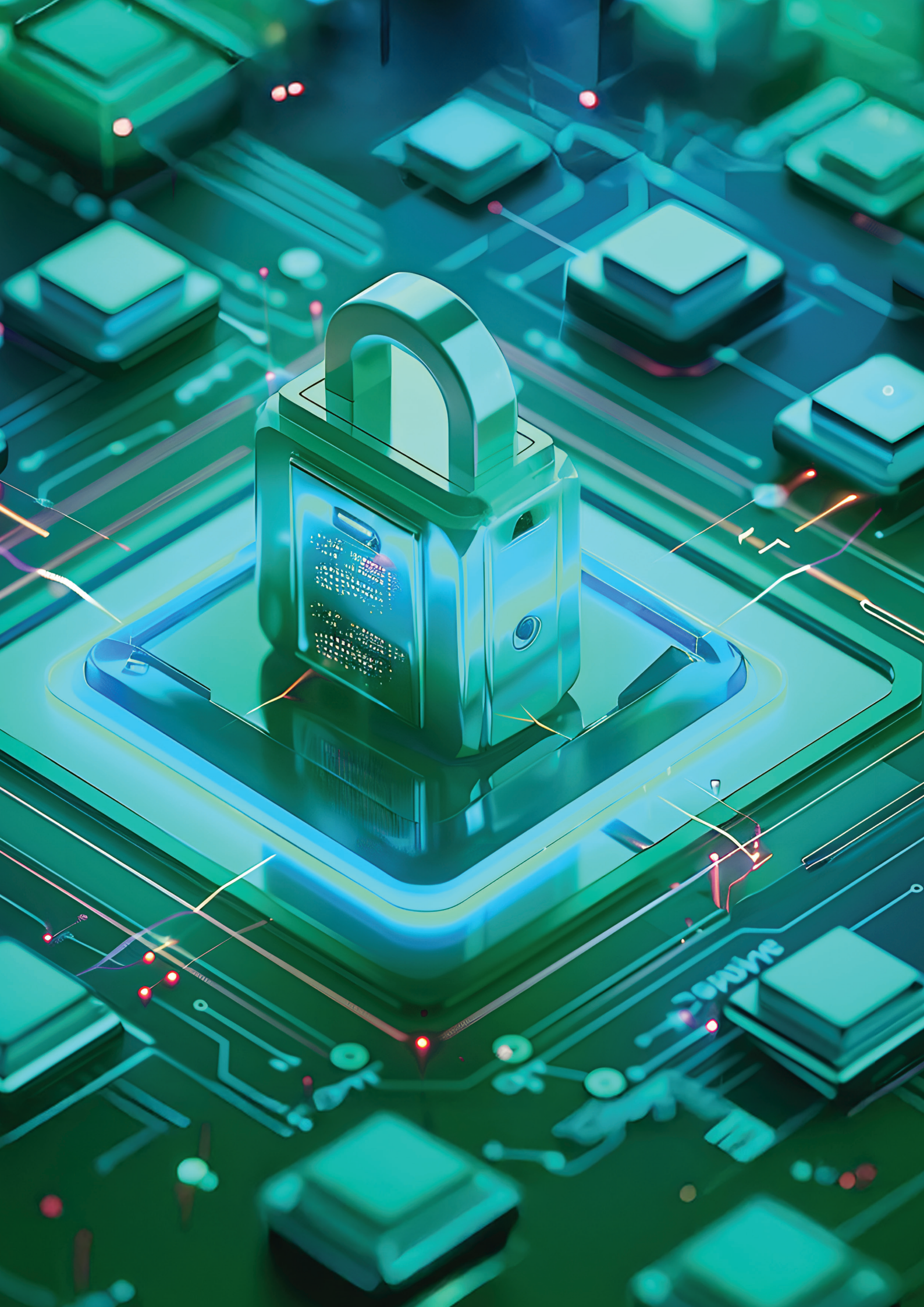
**Chiranth S**

**Arshad Mohammed**

**Priyanka Subburaman**

**Sanpreet Yadav**

**Mansi Agarwal**



Deloitte.