Deloitte.

India's Draft DPDP Rules
Leading digital privacy compliance

January 2025

Table of contents

Introduction

The notification of the Draft Digital Personal Data Protection Rules, 2025, published on 3 January 2025 ("draft Rules") marks the first major step towards establishing a comprehensive data protection regime in India since the enactment of the Digital Personal Data Protection Act, 2023 (DPDPA).[1] The draft Rules, issued by the Ministry of Electronics and Information Technology (MeitY), have been highly anticipated. Following several rounds of expert consultations over the past 18 months, the draft Rules provide much-needed clarity on many obligations organisations must fulfil under the DPDPA.

The draft Rules aim to establish a clear and structured framework that allows organisations to manage personal data responsibly while giving individuals better control over their personal data. But what do these draft Rules mean for companies that have already started preparing for India's data protection regime? Some stakeholders may find that the government's approach could benefit from clearer guidance, which would simplify data protection obligations. However, the key takeaway from the draft Rules is their incremental nature. Organisations that have already taken steps to protect personal data can make minor adjustments to their existing processes, which will significantly advance their readiness. The Rules reassure those in the early stages as they realign closely with global data protection trends and expectations.

Key coverage

The draft Rules outline the obligations of a data fiduciary in a manner that goes beyond the typical provisions found in other data protection regulations. In this point of view, we will discuss the following key aspects:

- The impact the draft Rules (read together with the DPDPA, IT Act and other laws in force in India) will have on different business functions and the key takeaways for leadership in driving readiness within their organisation.
- The typical journey towards data protection readiness and the areas where companies must make additional efforts to comply with the draft Rules.

The draft Rules are still in the proposal stage. Several rounds of public consultation could lead to revisions before the government issues the final version in the coming months.

Kindly note that the views presented are based solely on the published draft version of the Digital Personal Data Protection Rules, 2025, released on 3 January 2025.

[1]The Digital Personal Data Protection Act, 2023, available at the Ministry of Electronics & Information Technology website here https://www.meity.gov.in/data-protection-framework

What the draft Rules mean for you

1. Personal data breach notification

- Data breach management has long been a priority for India, even before the introduction of the DPDPA, as demonstrated by the comprehensive CERT-in Directions.[2] With the draft Rules, the DPDPA takes a significant step forward by ensuring that affected data principals are notified through their preferred communication channels. This is a commendable move towards fostering trust between data fiduciaries and data principals. The draft Rules also provide clear and detailed information on what must be communicated to the Data Protection Board of India, highlighting the need for a prompt and thorough investigation by data fiduciaries. Furthermore, the draft Rules aim to align with the CERT-In Directions by incorporating a two-step process, requiring immediate notification (to comply with CERT-IN) and a 72-hour window [3] to provide additional details. Overall, the approach to managing data breaches reflects the importance of a serious and thorough process.

2. Format for notice and consent

- 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 all sectors, ensuring communication is clear and accessible regardless of linguistic or technological barriers.

- The 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 all 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 Data Protection Board. This ensures a simple and straightforward process through multiple channels such as the website, email or phone.

[2]Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet, 28th April 2022, https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
[3]Section 7(2)(b) of the Draft Digital Personal Data Protection Rules, 3 January 2025. https://pib.gov.in/PressReleasePage.aspx?PRID=2090048.

3. 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,[4] the person who claims to be a parent or lawful guardian should submit appropriate documents to be eligible to provide consent on behalf of the children. It's important to consider the religion-based guardianship provisions outlined in various laws, including: The Indian Christian Marriage Act, 1872,[5] The Muslim Personal Law (Shariat) Application Act, 1937,[6] The Hindu Minority and Guardianship Act, 1956.[7]

  .

- To determine the scope of a person with a disability, one must submit appropriate documents of guardianship under the Rights of Persons with Disabilities Act, 2016[8] and National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999,[9] 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.

- User account maintenance is an additional obligation for the data fiduciary to keep a check on 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.[10]

[4]Guardians and Wards Act, 1890. Mar. 1890, http://indiacode.nic.in/handle/123456789/2318.
[5]Indian Christian Marriage Act, 1872. July 1872, http://indiacode.nic.in/handle/123456789/2186.
[6]Muslim Personal Law (Shariat) Application Act, 1937. Oct. 1937, http://indiacode.nic.in/handle/123456789/2303.
[7]Hindu Minority and Guardianship Act, 1956. Aug. 1956, http://indiacode.nic.in/handle/123456789/1649.
[8]Rights of Persons with Disabilities Act, 2016. Dec. 2016, http://indiacode.nic.in/handle/123456789/2155.
[9]National Trust for Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999. Dec. 1999, http://indiacode.nic.in/handle/123456789/1951.
[10]Rule 11 read together with Sr. No. 3 of Part B of the Fourth Schedule of the draft Rules, https://pib.gov.in/PressReleasePage.aspx?PRID=2090048

4. Reasonable security safeguards

- The draft 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 global practices 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 tools in data protection. The implementation must ensure that encryption protocols are up-to-date and strong enough to protect against evolving cyber threats.

- Reasonable security safeguards with mandatory baseline requirements offer organisations the flexibility to implement controls such as encryption and access controls based on their risk profile without prescribing specific standards if the baseline criteria are met.

- The draft Rules require visibility over access to personal data and early detection of unauthorised access. This can be achieved through Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) to restrict sensitive data access to authorised employees. With the rise of remote work and cloud environments, endpoint security should be prioritised through regular updates, patches and monitoring to address vulnerabilities and prevent breaches.

- The Data Fiduciary's DPO team should quickly notify the legal team about the latest amendments regarding reasonable security safeguards for contracts with data processors and fiduciaries. A standard clause incorporating these safeguards should be added to all contracts in line with the draft Rules.

5. 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 the 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 draft 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.

- Currently, for India, the Ayushman Bharat Health Account (ABHA)-Ayushman Bharat Digital Mission (ABDM) app currently serves as the closest equivalent to a Consent Manager.

6. Data retention

- This provision is significant as it emphasises 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.

- The draft Rules have considered three major data fiduciary classes: social media, e-commerce and online gaming. Additionally, data fiduciaries may also include OTT platforms, travel websites (with huge involvement of AdTech entities), 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.

- There is no mention of methods of secure disposal, archival and storage format of personal data. 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.

Implications for businesses: Realigning internally and defining responsibilities

Key insights for business leaders

The draft Rules present significant implications for organisations, particularly concerning compliance and personal data protection. Leaders must prioritise data protection as a fundamental organisational value, seamlessly integrating it into the overall business strategy. This will involve allocating sufficient resources to enhance IT infrastructure, implement robust data protection measures and foster a culture of accountability.

Leadership should also ensure that financial resources are directed towards advanced security tools, legal compliance, employee training and ongoing operational costs, such as Data Protection Impact Assessments (DPIAs) and audits (including vendor audits) for significant data fiduciaries.

The draft Rules will have specific implications across various departments within companies. Leadership will need to make critical decisions regarding budget allocation for compliance, team structures, the appointment of a Data Protection Officer (DPO) and realigning systems to align with DPDPA requirements.

Essential takeaways for leadership of distinct business functions, such as:

1. What this means for Human Resources (HR)

The draft Rules require data fiduciaries to obtain verifiable parental consent when processing children's data for insurance/ nominee purposes. Data must be collected only for specific, legitimate purposes, such as insurance. HR must ensure that it is retained only as long as necessary and securely erased thereafter. HR must adhere to the draft Rules on data retention and processing for employees and ex-employees, ensuring compliance with data minimisation and purpose limitation principles. Collaboration with legal and IT teams is essential to ensure the secure handling of sensitive data and maintain compliant consent management systems.

2. What this means for the sales and marketing team

The draft Rules will impact the sales and marketing team by requiring explicit, informed and revocable consent for data collection, necessitating updates to consent management processes. Organisations must ensure transparency in data usage and clearly communicate customer rights, which may affect customer trust. The draft Rules also require robust systems for data erasure, consent withdrawal and response to customer requests, along with enhanced data security measures to protect customer information. These changes will drive a more stringent and transparent approach to data handling, potentially influencing customer acquisition and retention strategies.

3. What this means for the IT department

Under the DPDPA, data protection is a continuous commitment requiring ongoing compliance efforts. IT and Information Security teams must implement the controls outlined in the draft Rules (encryption, tokenisation, access control, CIA triad, unauthorised access detection and data loss prevention) and adopt broader standards such as ISO 27001/27701. They must also establish systems for erasing personal data, managing consent transparently, verifying parental consent and integrating digital locker and consent management tools. The DPDPA 2023 places significant responsibilities on IT teams to innovate, upgrade systems and collaborate across departments. Additionally, IT must train the organisation on new systems and features to ensure compliance and smooth adoption of the DPDPA's requirements.

4. What this means for the legal department

The draft Rules shall also have significant implications for a legal department, requiring them to ensure the organisation's compliance with the draft Rules' detailed provisions. This includes reviewing and updating contracts with third parties, managing data subject rights with clear guidelines on communication and ensuring robust consent management systems with pre-set consent formats. The legal department will play a crucial role in mitigating risks associated with non-compliance, such as penalties, by working closely with IT, InfoSec and compliance teams to integrate data protection measures such as PbD and breach notifications. Additionally, the legal team will need to drive training and awareness across the organisation to ensure all employees understand their obligations under the new framework.

In conclusion, the DPDPA imposes significant obligations across multiple departments, requiring leadership, cross-departmental collaboration and a strong commitment to data protection. While India draws inspiration from global regulations such as the GDPR, it takes a unique approach to key compliance areas such as children's data protection, consent management and data breach notifications. As a result, Data Fiduciaries, even those compliant with international standards, must take specific actions to align with the DPDPA, necessitating a thorough reassessment of their data handling practices to ensure compliance with India's regulatory framework.

Way forward: The compliance road ahead

The DPDPA, 2023, and the draft Digital Personal Data Protection Rules, 2025, are guidelines for all data fiduciaries. Organisations now need to plan their compliance journey, keeping in mind the personal data processing guidelines in DPDPA, 2023, and draft Rules vis-a-vis their business use cases for processing personal data and where they fall in the compliance pyramid.

If your organisation has not yet prioritised privacy compliance, it is essential to take the following steps to initiate your DPDPA compliance journey:

- Identify all locations where personal data is stored across your organisation.
- Familiarise yourself with the applicability of the DPDPA and its draft Rules while considering any sector-specific requirements.
- Conduct a comprehensive privacy assessment to identify key areas that require immediate attention.
- Develop a compliance strategy and establish a provisional timeline for implementation.
- Organise orientation or introductory sessions for relevant stakeholders within your organisation.

Furthermore, if your organisation has already started its DPDPA compliance journey, it should focus on the following areas that may require additional guidelines:

- Incorporating process-level steps for breach notifications, communication, managing data principal rights, obtaining consent for processing children's personal data, etc.
- Internal restructuring of teams to manage additional responsibilities, such as coordination with the Data Protection Board of India, consent management and digital locker services.
- Conduct a reassessment beyond the existing assessment results to ensure compliance with the draft Rules, including communication and reporting mechanisms, notices or any other alignment per the draft Rules.
- Update technical security measures, such as the use of virtual tokens, in accordance with the suggestions under the draft Rules.

Each data fiduciary should view the compliance journey through the lens of their own company's specific needs. For example, if your company is already GDPR-compliant, you are already positioned higher on the compliance pyramid. However, you will still need to integrate DPDPA-specific elements such as using consent managers, managing data principal rights as specified under DPDPA and developing mechanisms to effectively notify Indian authorities of data breaches, among other requirements.

Connect with us

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

Deepa Seshadri
Partner and Leader – Cyber
Deloitte South Asia
deseshadri@deloitte.com

Gaurav Shukla
Partner
Deloitte India
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

Gaurav Khera
Partner
Deloitte India
gkhera@deloitte.com

Sowmya Vedarth
Partner
Deloitte India
sovedarth@deloitte.com

Contributors

Ketan Modh
Harsh Malviya
Jayati Garg
Ardhendu Sekhar Nanda

Acknowledgements

Apurva Chavan
Geetika Jain
Sarvesh Shahane
Yashasvani Vashisht
Sunita Kumari
Shreeti Nair
Neha Kumari

Deloitte.