DIGITAL PERSONAL DATA PROTECTION RULES, 2025

A SNAPSHOT

- The Ministry of Electronics and Information Technology (MeitY) has notified the Digital Personal Data Protection Rules, 2025 (DPDP Rules) on 13 November 2025, thereby initiating the process for operationalising the data protection framework envisioned under the Digital Personal Data Protection Act, 2023. MeitY has also issued notifications to bring key provisions of the DPDP Act into force and has set out phased implementation timelines over the next 18 months.

- Section 43A of the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 will remain in force until the end of 18-month period of implementation.

Timeline for Implementation

- From 13 November 2025: Rules 1 & 2 (Short Title, Definitions) and Rules 17-21 (Data Protection Board functions) are in immediate effect.

- After 12 months (by 13 November 2026): Rule 4 (Registration and Obligations of Consent Managers) becomes operative.

- After 18 months (by 13 May 2027): Rules 3 and 5-16, and 22-23 take effect, covering full set of obligations on Data Fiduciaries, notices, consent, rights, disclosures, children's data, cross-border transfers etc.

Key Provisions

- **Consent and Notice**

Under the DPDP Act, the Data Fiduciary is to serve a notice to the Data Principal prior to or accompanied with the request for consent. The DPDP Rules provide that the notice must comply with the following parameters:

- be provided with necessary details to enable Data Principal to give specific and informed consent which shall include, (a) Itemised description of such personal data; and (b) Specified purposes and description of goods or services or uses to be enabled, upon processing such personal data.
- be presentable and understandable independently of any other information, be given in clear and plain language.
- be provided with a specific communication link for accessing website or app (or both) of such Data Fiduciary and other means (if any) using which Data Principal may amongst others, withdraw the consent - ensuring that withdrawal is as easy as giving consent.

duadel@duaassociates.com
www.duaassociates.com
+ 91 11 2371 4408

Management of Consent – Consent Manager

The DPDP Act provides that the Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager.

The DPDP Rules set out the requirements and conditions for consent manager including for it to be an Indian company having net worth of not less than INR 20 million and having sufficient capacity, including technical, operational and financial, to fulfil its obligations as a Consent Manager.

The DPDP Rules also set out the manner in which consent is to be managed and the obligations/ requirements to be met by the Consent Manager – this includes, adoption of security safeguards, restriction on reading the content of personal data, no sub-contracting/ assignment and ensuring processes for regular audits and compliance.

Further, the Consent Manager must act in a fiduciary capacity towards the Data Principal and avoid conflicts of interest with Data Fiduciaries, including in relation to their promoters and key managerial personnel.

Reasonable Security Safeguards, Breach Notification and Retention

Reasonable Security Safeguards

As per the DPDP Act, a Data Fiduciary is obligated to protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.

The DPDP Rules further provides the measures which are considered as 'reasonable security safeguards' to be adopted by a Data Fiduciary at the minimum. These include, securing personal data using measures like encryption, obfuscation or masking, or virtual tokens; implementing appropriate access controls and keeping visibility on who accesses data; maintaining access logs for at least one year; monitoring and reviewing logs regularly; putting in place business continuity and recovery measures; ensuring flow down of security obligations to data processors through contracts; and implementing technical and organisational measures.

Breach Notification

In the event of a personal data breach the Data Fiduciary is to inform affected individuals 'without undue delay', describing nature of breach, consequences, remedial steps and contact for assistance (no timeline is prescribed). Additionally, the Data Fiduciary is to notify the Data Protection Board of India (DPB) as following: (a) without delay - first intimation with breach, location, time and extent, (b) followed by a report within 72 hours (or such other longer time as the DPB may approve upon the request of a Data Fiduciary) of becoming aware of the breach with detailed information.

Retention of data

Data is to be retained as follows:

- All personal data, associated traffic data, and certain logs are to be retained for at least one year for specified purposes (such as responding to lawful requests or supporting investigations). After this period, such data must be erased unless another law requires longer retention.
- Large fiduciaries like e-commerce entities, online gaming intermediaries, and social media intermediaries above specified thresholds (in term of the number of registered users) need to erase data after 3 years of user inactivity.
- A 48-hour pre-deletion notice is to be given before any erasure.

Data of Children and persons with disabilities

As per the DPDP Act, prior to processing personal data of child or a person with disability, the Data Fiduciary is mandated to obtain verifiable consent from the parent or lawful guardian.

Children's data

The DPDP Rules require a Data Fiduciary to adopt appropriate technical and organisational measures and undertake due diligence to ensure that verifiable consent of the parent is obtained before the processing of any personal data of a child, using reliable age and identity verification methods. Parents may identify themselves either from records already held by the Data Fiduciary or by providing government-issued identity/age details or a virtual token, including via a Digital Locker service provider.

Data of Persons with disability

For persons with disabilities who have a lawful guardian, the Data Fiduciary must verify that the guardian has been formally appointed under applicable laws such as the Rights of Persons with Disabilities Act, 2016 or the National Trust Act, 1999.

Exemptions

Certain Data Fiduciaries are exempt (from age verification/ not undertaking tracking or behavioural monitoring) when processing a child's data strictly for safety or health-related purposes. These include: (a) healthcare establishments and professionals, who may process data only to provide or support necessary health services, (b) Educational institutions, crèches and day-care providers may process data for educational activities, tracking or behavioural monitoring to ensure children's safety, and (c) Transport providers engaged by such institutions may process location data solely to ensure the child's safety.

These exemptions are also applicable in case of processing of personal data of a child for specified purposes such as providing any subsidy, benefit or service in the interests of child.

Cross-Border Data Transfers & Localisation

The Data Fiduciary may transfer personal data outside India subject to the restriction that the Data Fiduciary shall meet such requirements as the Central Government may, by general or special order, specify in respect of making such personal data available to any foreign State or any entity under its control or authority. This may create challenges for Data Fiduciaries in reconciling with the conflicting obligations under laws of other countries.

Significant Data Fiduciary

As per the DPDP Act, certain classes of Data Fiduciary are considered as "Significant Data Fiduciary" (SDF). Such Significant Data Fiduciary have additional obligations in contrast to ordinary Data Fiduciary. The DPDP Rules require the SDF to: (a) conduct a Data Protection Impact Assessment and an audit (through an independent auditor) every 12 months and submit a report to the DPB, (b) verify that technical measures, including algorithmic software used to host, display, upload, modify, publish, transmit, store, update, or share personal data, do not pose likely risks to data principals' rights, and (c) comply with Government's directions on data transfer outside of India.

If the Central Government identifies certain categories of personal data as "restricted for transfer," the SDF must ensure that the said personal data, and the traffic data related to its flow, are not transferred outside India. This opens the room for possible localisation requirements. The SDF must verify that all technical measures and algorithmic systems it uses—including those for hosting, display, uploading, publishing, transmission, storage, updating, or sharing of personal data—do not pose risks to the rights of Data Principals.

Timeline for Grievance Redressal

The DPDP Rules require that grievances of the Data Principals are resolved within 90 days by Data Fiduciaries/ Consent Manager.

Immediate Action Points for companies

- Gap Assessment and alignment: Mapping of personal data being collected and processed within the organisation, including the types of personal data being collected, processes for collection and processing the personal data, the purpose for which the data is being collected and aligning it with the DPDP Act and the DPDP Rules.

  Specifically, the following key aspects would need to be looked into:

- Create a DPDP Compliance Implementation Roadmap
- Consent management: Implement systems to manage consent, withdrawals and erasure.
- Providing for norms on purpose limitation and data minimization. Draft Data Retention and Deletion Policies
- Plan for Consent Manager Integration
- Establish a Data Breach Response System
- Policies and Notices: Review and put in place all notices, privacy policies and related processes and mechanisms.
- Security Standards: Implement security safeguards.
- Special Category Data: Enable norms for processing personal data of children and persons with disabilities.

- Training and Awareness: Brief all employees on handling 'Personal Data' under the new regime. Given the significant penalties, risks and obligations should be clearly understood.

- Contract Management: Review and update all contracts with vendors, processors to include DPDP Act related obligations and compliances.

There is no uniform or generic approach for adoption of the DPDP Act and DPDP Rules.
A phased compliance tailored to the specific sector and scale will need to be undertaken.

About Us

Dua Associates is a full-service national law firm with a dedicated Technology, Media and Telecommunications (TMT) practice group. We have an expert team to guide clients through all nuances, practical and technical, related to the implementation of the DPDP law.

We bring a unique blend of policy insight and practical legal expertise — including former senior Government officials (also being a member of the Data Protection Committee formed to frame the existing privacy law) as well as lawyers with deep sectoral experience.