Regulatory Insights

4 January 2025

Draft Digital Personal Data Protection Rules, 2025 released – open to public comments

In brief

The Government of India had introduced the Digital Personal Data Protection Act, 2023 (DPDP Act)[1] in 2023 with the objective of regulating the processing of digital personal data, the rights and duties of individuals (Data Principal) and obligations of organisations (Data Fiduciaries) to use or process personal data.

On 3 January 2025, the Ministry of Electronics and Information Technology released the draft[2] of the Digital Personal Data Protection Rules, 2025 (Draft Rules) under the DPDP Act, inviting feedback or comments from the public. The deadline to submit the comments is 18 February 2025.

In detail

Key highlights of the Draft Rules

In this Regulatory Insights we have captured the key highlights of the Draft Rules that are enumerated below.

1. Phased implementation (Rule 1)

Certain rules shall come into effect in a phased manner, which means that different provisions will come into effect on different dates upon notification by the government. This will allow Data Fiduciaries to adapt to this new data privacy framework smoothly.

Impact: For sectors that heavily rely on personal data and require complex compliance measures, it appears that the government may grant additional time, allowing them to prepare and adapt to the regulatory requirements.

2. Notice requirements (Rule 3)

Data Fiduciaries must provide the necessary information to enable the Data Principal to give specific and informed consent. Such notice must be clear, standalone, in simple language and must include the following particulars –

- Itemised list of personal data being collected;
- The specific purpose for which such personal data is collected;
- Itemised description of goods and/ or services to be provided by such collection of personal data;

  Link for accessing the website or app, or both, of the Data Fiduciary; and
- Description of how the Data Principal can withdraw her consent, exercise her rights under the DPDP Act and file a complaint with the Data Protection Board of India (Board).

As a result, companies must review and modify the existing notice format (if any) or alternatively draft a new

1 The DPDP Act received the assent of the President and was published on 11 August 2023.
2 Notification No. G.S.R. 02(E) dated 3 January 2025

notice and provide the same to Data Principals in the future before collecting their personal data. Additionally, it is to be noted that the obligation of providing the notice is retrospective. Accordingly, a notice to existing Data Principals must be issued as soon as practically possible.

Impact: These provisions are already outlined in the DPDP Act; however, the Draft Rules offer clarity by elaborating on the specific obligations and providing guidelines for compliance.

3. Registration and obligations of a Consent Manager (Rule 4)

Consent Mangers are companies with interoperable platforms that act as a single point of contact to enable a Data Principal to give, manage, review and withdraw consent to Data Fiduciaries onboarded onto such platforms.

Consent Managers are required to be registered with the Board. The conditions for registration are mentioned below.

- The company should be incorporated in India;
- It should have sound and financial operational activity with a minimum net worth of INR 20 million;
- It should have a reputation for fairness and integrity in its management; and
- A certified interoperable platform is required, enabling Data Principals to manage their consent.

Impact: This will enable companies to facilitate interoperable platforms that act as a single point of contact, allowing Data Principals to give, manage, review, and withdraw consent to Data Fiduciaries onboarded on such platforms. For organisations handling significant amounts of personal data, a Consent Manager is required for addressing the following obligations –

- Maintaining records of consent requests and consents given, denied or withdrawn by Data Principals. Access to these records must be provided to the Data Principals, and they should be retained for (i) at least seven years, (ii) for a longer duration as mutually agreed upon by the Data Principal and Consent Manager, or (iii) as required by law.
- Prohibiting the sub-contracting or assignment of its obligations under the law.
- Prohibiting the transfer of control of the Consent Manager company, such as through a sale or merger, without prior consent from the Board.
- Conducting periodic audits and sharing the outcomes of these audits with the Board.
- Publishing key management details and ownership structures on the company's website or app to ensure transparency and avoid conflicts of interest.

4. Reasonable security safeguards (Rule 6)

Every Data Fiduciary will protect the personal data in its possession by taking reasonable security safeguards such as encryption, obfuscation, masking, control access on a needs basis, detection of unauthorised access and by implementing robust clauses in the contracts entered into between a Data Fiduciary and a Data Processor[3] to ensure effective observance of security safeguards.

5. Intimation of personal data breach (Rule 7)

a. **Intimation to affected Data Principals:** Upon becoming aware of a personal data breach, the Data Fiduciary must, without delay, notify the affected Data Principals through their registered communication mode. Such notification should provide the following particulars –

   - Brief details of the breach;
   - Likely consequences relevant to such Data Principal;
   - Mitigation measures being undertaken by the Data Fiduciary;
   - Recommended safety measures for such Data Principals; and
   - Business contact information of the Data Fiduciary for handling the queries of the affected Data Principals.

[3] Data Processor means any person who processes personal data on behalf of a Data Fiduciary.

b. **Intimation to the Board:** The Data Fiduciary must also inform the Board without delay, detailing the breach and its likely impact. Moreover, within 72 hours or within such longer period as the Board may permit, the Data Fiduciary is required to submit the below mentioned to the Board.

- Detailed updated findings of the breach;
- Implemented or proposed mitigation measures;
- Findings about the person who caused the breach;
- Remedial measures to prevent recurrence; and
- Report on the intimation provided to the affected Data Principals.

Impact: A Data Fiduciary will have to frame or update its personal data breach mechanism or framework to ensure effective observance of the DPDP Act and Rules framed thereunder.

6. Erasure of personal data by certain classes of Data Fiduciaries (Rule 8)

If certain classes of Data Fiduciaries processing personal data for purposes as listed in the table below do not engage with a Data Principal for a specific period of time, then it must erase the personal data of such Data Principal, unless required for legal compliance. Before erasing such data, the Data Fiduciary is required to notify the Data Principal at least 48 hours in advance that their data will be erased unless they login to their account or initiate contact again with the Data Fiduciary.

Classes of Data Fiduciaries	Purposes	Time period
• E-commerce entity having not less than 20 million registered users in India • Online gaming intermediary having not less than 5 million registered users in India • Social media intermediary having not less than 20 million registered users in India	For all purposes, except for the following: • Enabling the Data Principal to access her user account; and • Enabling the Data Principal to access any virtual token that is issued by or on behalf of the Data Fiduciary, is stored on the digital facility or platform of such Data Fiduciary, and may be used to get money, goods or services	Three years from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest.

Impact: Data Fiduciaries would be required to send notices to inactive users and delete their personal data if there is no response. This compliance requirement will also ensure reduction of the volume of stored data, potentially affecting operations such as marketing and analytics. Additionally, it may require adjustments to data management systems to ensure proper identification and deletion of inactive user data.

7. Information to be published by Data Fiduciaries (Rules 9 and 13)

Every Data Fiduciary and Consent Manager must prominently mention the following particulars on its website or app –

- Business contact information for addressing the queries which the Data Principal may have with respect to their personal data being processed;
- Clear procedure and details as to how a Data Principal can exercise her rights (such as the right to correct and erase personal data) under the DPDP Act; and
- Period within which the Data Fiduciary or Consent Manager will respond to the grievances of the Data Principals.

Impact: The information and policies mentioned on the website and/ or apps are required to be updated and aligned to the DPDP Act and rules framed thereunder.

8. Verifiable consent for processing personal data of children and persons with disabilities (Rules 10 and 11)

A Data Fiduciary is required to implement measures for obtaining verifiable consent from parents or lawful guardians before processing the personal data of a child or a person with disability. Moreover, due diligence should be observed in checking that the individual identifying as the parent or lawful guardian is an adult and

that the guardian is appointed by a court, designated authority or local committee under the applicable guardianship law.

A Data Fiduciary can obtain verify the parent's or lawful guardian's age and identity *via* the following means –

- Reliable identity and age details already held by the Data Fiduciary; or
- When such parent or lawful guardian voluntarily provides details of her identity and age or a virtual token mapped to the same, which is issued by a government entity (such as details or token verified and made available by a Digital Locker service provider).

Exceptions from this requirement, along with the requirement to not undertake tracking or behavioural monitoring of children or targeted advertising directed at children, apply to classes of Data Fiduciaries such as educational institutions, clinical establishments, mental health establishments and healthcare professionals, subject to certain conditions. Exceptions also apply for specific purposes, including processing children's data to ensure detrimental information is not accessible to a child or for creating a user account for email communication, subject to certain conditions.

Impact: Seeking verifiable parental consent can help companies stay compliant with privacy laws, protect children's data and build trust with parents. However, it also poses challenges such as additional operational costs, potential barriers to user acquisition and limitations on data collection, all of which companies need to navigate strategically.

9. Other key highlights of the Draft Rules

- **Rules 5 and 15:** The state and any of its instrumentalities may process the personal data of a Data Principal to provide or to issue to her any subsidy, benefit, service, certificate, license or permit, and will adhere to certain technical and organisational measures while processing such data. Additionally, the provisions of the DPDP Act will not apply to the processing of personal data necessary for research, archiving or statistical purposes if it is carried on in accordance with certain standards.
- **Rule 12:** Significant Data Fiduciaries[4] are mandated to conduct a Data Protection Impact Assessment and a comprehensive audit once a year and share the results of these assessments with the Board. Moreover, Significant Data Fiduciaries will ensure that certain personal data and traffic data, as specified by the Central Government, are not transferred outside India.
- **Rule 14:** Data Fiduciaries must comply with any requirements that the Central Government sets in respect of transferring personal data to foreign states and entities.

The takeaways

The Draft Rules offer clearer guidance to support the implementation of the DPDP Act. Enhanced measures are included to protect individuals' digital personal data, emphasising the importance of consent and lawful processing. Exemptions are provided for data processing conducted for research, allowing such activities to proceed with the necessary safeguards to protect personal data. The Draft Rules exclude non-personal, personal data in physical format and anonymised data from the scope of the regulations, focusing solely on digital personal data protection.

[4] Significant Data Fiduciary means any Data Fiduciary, or a class of Data Fiduciary, as may be notified by the Central Government.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 360,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Follow us on

Facebook, LinkedIn, Twitter and YouTube.

KA-September 2024-M&C 40853