Deloitte.

Tax alert: Draft Digital Personal Data Protection Rules, 2025

6 January 2025

On 3 January 2025, the Central Government published draft rules outlining several aspects such as publication of notice, data deletion timelines for certain categories of Data Fiduciaries, data localization requirements and the functioning of the regulatory body - the Data Protection Board ("DPB"). The draft rules have been issued for public consultation and comments can be provided till 18 February 2025.

In a nutshell

Notice and Breach Reporting-

Notice needs to provide itemized description in a clear and plain language to the Data Principal

- Personal data being collected.
- Specified purpose for use of the data
- Goods and services which will be offered.

Personal Data Breach Reporting-The Data Fiduciary must inform the Data Principal and Data Protection Board ("DPB") about any personal data breach without delay and also provide additional details about the breach within 72 hours.

E-commerce entities, online gaming intermediaries and social media platforms having minimum registered users, are required to erase personal data within 3 years from the last interaction / request from data principal or implementation of DPDP rules whichever is later.

Child data – Verifiable consent mechanism provided for processing child data. Exemption has been provided for class of Data Fiduciaries in healthcare and education for defined purposes.

Significant Data Fiduciaries need to ensure that the algorithmic software deployed does not pose risk to data principal rights; certain classes of SDF may need to store specified personal data within India.

Reasonable security standards such as minimum technical standards and measures such as encryption, access control, log monitoring, masking, security standards prescribed, including maintaining logs for one year.

Scroll down to read the detailed alert

Key highlights of the Draft Digital Personal Data Protection Rules, 2025 ("Rules")

- **Introduction to the Rules-** The Central Government, in exercise of its powers under sub-section (1) and (2) section 40 of the Digital Personal Data Protection Act, 2023 ("Act"), has published Rules for public consultation till 18 February 2025. The Rules compliment the Act and provide a detailed understanding of aspects such as rights of data principals, exemptions to be provided to Data Fiduciaries, processing of personal data outside India, to name a few.

  It is stated that Rules 3 to 5, 21 and 22 shall come into force on the date specified by the Central Government. The remaining Rules (dealing with board establishment and appeal procedure) shall come into force on the date of their publication in the Official Gazette. Additionally, the Rules state that all expressions shall have the same meaning as ascribed to them in the Act.

- **Notice-** This provides the manner for a notice to be published by the Data Fiduciary. The **language must be clear, simple, in plain language and understandable** by the data principal. It also states that the notice should include an itemized list of the personal data being collected and processed along with detailed description of goods and services or uses authorized by such processing.

  Additionally, a communication link should be published by the Data Fiduciary, which shall be available on their application or on the website for the Data Principal to withdraw consent, exercise their rights and lodge a complaint with the Board on any grievances.

- **Reasonable security safeguards-** Some key measures to be taken by Data Fiduciaries for implementing reasonable security measures to protect personal data, are as follows:

  — Maintenance of appropriate logs, measures for detecting unauthorized access, retain logs for a period of 1 year.

  — Appropriate encryption, access control and data back-ups

  — Contractual obligations on the Data Processor to ensure taking appropriate security safeguards.

  — Access control to the computer resources in use by Data Fiduciaries and Data Processors

- **Intimation of personal data breach -** The Data Fiduciary must inform the DPB about any personal data breach without delay, and details regarding the breach need to be reported within 72 hours or within the stipulated time-period as the DPB may allow on request. Additionally, the Data Fiduciary is obligated to inform data principals to the best of their knowledge of any personal data breach. However, the Rules do not specify any timeline for intimation to the Data Principals. Some key aspects to be covered by the Data Fiduciary are as follows-

  — The broad facts related to the events, circumstances and reasons leading to the breach.

  — Measures implemented or proposed, if any, to mitigate risk

  — Any findings regarding the person who caused the breach.

  — Remedial measures taken to prevent recurrence of such breach.

  — Report regarding the intimations given to affected Data Principals.

- **Time period for specified purpose to be deemed as no longer being served-** Rule 8 and the Third Schedule outline the different classes of Data Fiduciaries and specify that if the Data Principal does not engage with the Data Fiduciary within a specified period, the personal data must be erased unless required for legal compliance.

Retention periods have also been prescribed for certain classes of Data Fiduciaries:

Class of Data Fiduciary	Purpose	Time Period
E-commerce Entity (having more than 2 crore registered users)	For all purposes (except (i) enabling data principal to access their user account; (ii) access any virtual token that may be used to avail money, goods, and services.	3 years from the last date of activity by data principal or the commencement of the DPDP Rules 2025, whichever is latest
Online Gaming Intermediary (having more than 50 lakh registered users)	For all purposes (except (i) enabling data principal to access their user account; (ii) access any virtual token that may be used to avail money, goods, and services.	3 years from the last date of activity by data principal or the commencement of the DPDP Rules 2025, whichever is latest
Social Media Intermediary (having more than 2 crore registered users)	For all purposes (except (i) enabling data principal to access their user account; (ii) access any virtual token that may be used to avail money, goods, and services.	3 years from the last date of activity by data principal or the commencement of the DPDP Rules 2025, whichever is latest

The Data Fiduciary shall notify the Data Principal that their data shall be erased at least 48 hours before the completion of the time period specified under this rule.

- **Verifiable consent for processing personal data of children and persons with disabilities -** Rule 10 requires Data Fiduciaries to implement appropriate technical and organisational measures to ensure that verifiable consent is obtained from a parent before processing a child's personal data. Data Fiduciary must verify the identity and age of the parent through reliable records or a verified digital token, issued by a government authorized entity or verified and made available by a Digital Locker service provider. Additionally, when seeking consent from a guardian of a person with a disability, the Data Fiduciary must confirm that the guardian is legally appointed by a court, authority, or committee, ensuring compliance with relevant laws on guardianship.

  The rules say that the following entities are allowed to carry out behavioral monitoring of a child and process children's data without verifiable consent:

  — Clinical establishments, mental health, and healthcare professionals: Restricted to providing health services to the child. Healthcare establishments must limit their processing activity to the protection of the child's health only.

  — Allied healthcare professionals: Restricted to supporting the implementation of a healthcare treatment and referral plan recommended by a healthcare professional.

  — Educational institutions: Restricted to tracking and behavioral monitoring of educational activities and in the interest of the safety of a child enrolled with them.

  — Crèche or childcare centers: Restricted to tracking and behavioral monitoring in the interest of the child's safety.

  — Transport services for educational institutions, creches and childcare centers: Restricted to tracking the location of the child during the course of their travel to and from the above-listed locations, in the interest of the child's safety.

  — For the exercise of any power, performance of any function or discharge of any duties in the interest of a child under law.

- Anyone entrusted under any law in force to perform any function or discharge any responsibility in the interest of the child.
- Providing or issuing subsidies, benefits, certificates, and licenses (To the extent necessary for providing the above-listed services).
- For creating an email account.
- To ensure that children cannot access information that is detrimental to their well-being.
- To confirm age of individual: Data Fiduciary may process personal data/conduct behavioral monitoring to confirm that the person whose data they are processing is not a child.

- **Additional Obligations of Significant Data Fiduciary –** Rule 12 chalks out additional obligations for organizations notified as Significant Data Fiduciaries ("SDFs") mandating them to conduct Data Protection Impact Assessment ("DPIA") and Audit once in every twelve months to ensure adherence to the Act and Rules made thereunder. The result of such DPIA/Audit (entailing key observations) is required to be furnished to the Board.

  Interestingly, the Rules require SDFs to verify that the algorithmic software used by them to inter alia process, host, display, publish and transmit personal data does not pose risk to the rights of the Data Principal. The Rules empower central government to impose data localization obligations on SDFs mandating them to store specific categories of personal data, as specified by the central government, within India's borders.

- **Rights of Data Principal –** Data Fiduciaries and Consent Manager (if applicable) are required to publish, on their website/app, the details of the process through which Data Principal can exercise their rights provided under the Act, including username/any other identifier to facilitate identification. Data Access/Erasure requests can be made by Data Principal by following the process published by Data Fiduciary. Additionally, Data Fiduciaries are also required to publish clear timelines for grievance redressal and implement technical and organizational safeguards to effectively respond to Data Principal's grievances. Data Principals can nominate one or more individuals to exercise their rights provided under the Act, following the process published by the Data Fiduciary and in accordance with the terms of service of the Data Fiduciary and extant applicable law.

- **Processing of personal data outside India –** Rule 14 outlines that personal data processed by a Data Fiduciary, whether within India or abroad (in connection with any activity related to offering of goods or services to Data Principals situated in India) cannot be transferred to a foreign country unless certain requirements set by the central government are met. The Data Fiduciary must comply with government-mandated requirements regarding the transfer of such data to foreign states or entities/agencies under their control.

- **Consent Manager –** Rules have provided additional clarity on the role of consent manager. A Consent Manager should be a company incorporated in India, having a minimum net worth of INR 2 crore and a platform enabling Data Principals to manage their consent preferences. All Consent Managers need to be registered with the Data Protection Board. Post registration, the Consent Manager must comply with obligations of ensuring that Data Principals can easily give, manage, review, and withdraw consent for data processing, maintaining records of consents and data sharing, and providing transparent access to such records. Critically, the Consent Manager needs to ensure that they do not have any access (even viewing access) to personal data.

- **Calling for information from Data Fiduciary or intermediary –** This provision grants the Central Government the authority to request information from Data Fiduciaries/Intermediaries for specific purposes outlined in the Seventh Schedule, which include safeguarding India's sovereignty, integrity, and security, fulfilling legal obligations, as well as assessing the status of Data Fiduciaries for notifying them as SDFs. The government may set a deadline for providing the requested information and, in cases where disclosure of information might harm the sovereignty and integrity of India, may require the Data Fiduciary/Intermediary to obtain prior written consent before sharing such information.

The rules have been notified for public consultation and any objections or suggestions may be submitted on the website of MyGov (https://mygov.in), on or before 18 February 2025.

Comments

The publication of the Draft Digital Personal Data Protection Rules, 2025 marks a significant step toward operationalising the provisions outlined in the Act. As privacy concerns and data security continue to be a focal point globally, these Draft Rules present a critical regulatory framework for businesses, technology providers, and consumers alike. Organizations need to start analyzing their internal systems, processes, contracts, and policies to understand their compliance with the DPDP Act and DPDP Rules, and work to build a privacy centric framework.

Deloitte.