DRAFT DIGITAL PERSONAL DATA PROTECTION RULES, 2025

INTRODUCTION

The Ministry of Electronics a nd Information Technology ("**MeitY**") published a draft of the Digital Personal Data Protection Rules, 2025 ("**Draft Rules**"), on January 3, 2025, in furtherance of the Digital Personal Data Protection Act, 2023 ("**DPDP Act**"). Certain provisions of the DPDP Act, which received presidential assent on August 11, 2023, required supplemental rules to allow for the intent of such provisions to be effected. This legislative framework, which is expected to come into effect pursuant to the consultation period, intends to operationalize India's commitment to safeguarding digital privacy while ensuring that data handling processes are lawful, transparent, and secure.

APPLICABILITY

The DPDP Act and the Draft Rules shall apply to the processing of digital personal data[1], whether processed in India or outside India but in connection with any activity relating to goods or services being offered to individuals in India. Any compliance obligations arising out of DPDP Act and the Draft Rules will fall upon any organisations that process data, including data fiduciaries (i.e. any person that determines the purpose and means of processing the personal data of individuals) and data processors (i.e. means any person who processes personal data on behalf of a data fiduciary).

The individuals whose personal data is collected and processed by fiduciaries are defined as being 'data principals' under the DPDP Act. The Draft Rules further elucidate the rights of data principals and the duties of data fiduciaries that are preliminarily captured in the DPDP Act.

KEY FEATURES OF THE DRAFT RULES

Obligations of data fiduciaries

- Notice requirements for data fiduciaries: Section 5 of the DPDP Act requires data fiduciaries to provide notices to data principals including information such as the personal data being sought and the purpose for which the same will be processed, and the rights of data principals in relation to the same. Rule 3 of the Draft Rules stipulates that such notices must be clear and understandable, independent of any other information, with an itemised description of personal data proposed to be processed. Informed consent is fundamental to this provision, as is also apparent from a bare reading of Section 6(1) of the DPDP Act which requires consent to be free, specific, informed, unconditional and unambiguous. The notice must also:
    - provide accessible communication links to the data fiduciary's platform;
    - describe the means to withdraw consent, which process must be comparable to the ease with consent is sought;
    - describe the means by which a data principal may exercise his/her rights under the DPDP Act; and
    - the manner in which a grievance may be escalated to the Data Protection Board ("**DP Board**").

[1] Section 2 (t) of the DPDP Act - "personal data" means any data about an individual who is identifiable by or in relation to such data.

- Reasonable security safeguards: Section 8 of the DPDP Act, mandates all data fiduciaries to take 'reasonable security safeguards' to prevent personal data breach. Rule 6 of the Draft Rules further elaborates the foregoing and requires data fiduciaries to implement security measures to protect personal data, including measures such as encryption of data, access control, monitoring for unauthorized access, and regular data backups. Contracts with data processors, must have appropriate provisions to ensure that these security standards are followed by such data processors.

- Data breach notification: In the event of a personal data breach[2], data fiduciaries are obligated to notify each affected data principal and the DP Board of such breach.[3] Rule 7 prescribes the manner in which such communication must be made to data principals and the DP Board as follows:
    - To data principals: Details of the breach, its consequences, the actions being taken to mitigate it must be provided, safety measures that the data principal may take to protect his/her interests, and details of a person who shall respond to any queries of the data principals on behalf of the data fiduciary;
    - To the DP Board: Details of the breach, its consequences, and the actions being taken to mitigate it, any findings regarding the person who caused the breach, and a report regarding the intimations given to affected data principals must be provided within 72 hours of detection (or a longer period, if authorized), along with a comprehensive account of the incident.

  While the Draft Rules set a 72 hour deadline for reporting a data breach to the DP Board, this timeline does not apply to data principals, who must be informed "without delay."

- Data retention policies: Section 8 of the DPDP Act requires data fiduciaries to erase personal data upon the earlier of (i) a data principal withdrawing their consent, or (ii) as soon as it is reasonable to assume that the specified purpose is no longer being served. Schedule 3 to the Draft Rules further identifies certain classes of data fiduciaries and data retention mandates in relation to the personal data processed/retained by them. The classes of data fiduciaries identified under the Draft Rules are as follows:
    i. e-commerce platforms with over 2 crore registered users in India,
    ii. online gaming intermediaries with over 50 lakh registered users in India, and
    iii. social media platforms with more than 2 crore registered users in India.

  The data fiduciaries falling within the threshold stated hereinabove must erase user data after 3 years of the data principal last approaching the data fiduciary, unless the user continues to maintain their account with such data fiduciary. The data fiduciary is required to notify the data principal at least 48 hours before the retention period ends, informing them that their data will be deleted unless they take action or exercise their rights regarding the processing of their data.

- Verifiable Consent for Processing Personal Data of Children and Persons with Disabilities: Section 9 of the DPDP Act sets out the requirement for obtaining verifiable consent from parents

[2] Section 2 (u) of the DPDP Act
[3] Section 8 (6) of the DPDP Act

of children or lawful guardians of persons with disabilities[4] before processing the personal data of children or persons with disabilities. It mandates that data fiduciaries must ensure that such consent is obtained and specifies the prohibition on tracking the behaviour of children for commercial purposes and any processing that is likely to cause any detrimental effect on the well-being of a child. Rule 10 of the Draft Rules provides the detailed framework for implementing this requirement. It specifies the measures data fiduciaries must take to verify the identity and age of the parent before processing a child's data. This verification can be done using reliable identity details or a virtual token issued by an authorized government entity, such as a Digital Locker service provider. It further requires a data fiduciary to observe due diligence to verify whether the guardian of a person with disability is lawfully appointed. However, Rule 11 exempts data fiduciaries such as healthcare providers, educational institutions, and those offering childcare services from complying with the requirements of obtaining verifiable parental consent, allowing them to process children's data for essential services like health, education, safety, and transportation tracking. The exemptions are accompanied by certain conditions and data processing activities must be limited to what is necessary for the child's well-being and protection, with strict emphasis on the child's best interests.

- Additional obligations for significant data fiduciaries: The central government is empowered to notify any data fiduciary or certain classes of data fiduciary as 'significant data fiduciaries'.[5] Further, Section 10 of the DPDP Act requires a significant data fiduciary to undertake periodic Data Protection Impact Assessment and audit to assess the implementation of the DPDP Act and the accompanying rules. Rule 12 specifies that such assessment and audit shall be conducted annually and a report containing significant findings from the assessment and the audit conducted must be furnished to the DP Board.

- Rights of data principals: Rule 13 requires data fiduciaries and consent managers (as applicable) to publish on the respective websites and/or apps the rights available to data principals under the DPDP Act and the accompanying rules, along with details to enable the data principals to exercise such rights.

- Transfer of personal data: Data fiduciaries transferring any personal data, the processing of which is governed by the DPDP Act and the Draft Rules must adhere to any restrictions set forth by the central government regarding the disclosure of such personal data to a foreign state or entities. Rule 14 does not prescribe any restrictions, but it must be noted that such restrictions may be introduced by general or special orders of the government.

Consent managers

- The DPDP Act introduced a 'consent manager'[6], as a single point of contact for data principals to give, manage, review and withdraw their consent. Rule 4 read with Part A, Schedule 1 of the Draft Rules further expands on the provisions for consent managers by specifying the requirements for a person to apply for registration as a consent manager, such as the volume of business and the

[4] Rule 10 of the Draft Rules
[5] Section 10 of the DPDP Act
[6] Section 6 (7) of the DPDP Act

net worth threshold. A company that fulfils such requirements for registration, may apply to the DP Board, proposed to be established in furtherance of the DPDP Act for the registration. Upon being granted registration, consent managers shall have obligations detailed under Part B of Schedule 1 of the Draft Rules, which include providing a platform to data principals to manage consent, maintaining a website or which the data principal can access the consent manager's services, having prescribed audit mechanisms etc.

Data Protection Board

- Section 18 of the DPDP Act lays down the framework for the establishment of the DP Board, which shall be a body corporate, for dealing with instances of data breach and violations of the DPDP Act. The appointment of members of the DP Board, terms and conditions of service by the members, and operations of the DP Board are detailed in Rules 16 through 20. The DP Board shall function as a digital office and adopt techno-legal measures to conduct proceedings as provided under the DPDP Act and the Draft Rules.

Powers of the government

- Data processing by the state: the state and their agencies are authorized to process personal data for purposes constituting legitimate use as per Section 7 of the DPDP Act. Rule 5 read with Schedule 2 to the Draft Rules prescribes standards for processing data in relation to providing subsidies, benefits, services, certificates, licenses, or permits, as defined by law or funded through public resources. Such processing must be lawful, transparent, secure, and limited to the necessary data for these purposes. Additionally, the government is exempt from obtaining user consent for processing personal data in foregoing situations.

- Disclosures to the central government: Rule 22 of the Draft Rules empowers the central government to request information from data fiduciaries or intermediaries for specified purposes, such as protecting the sovereignty, integrity, and security of India. However, there is lack of clear procedural guidelines for notifying data fiduciaries of these requests and for determining the specified time period for providing the information. Additionally, there are no defined safeguards for data security when the government handles such information, and no clarity on how long the data will be retained or its intended use.

Exemption for processing of data for research and statistical purposes

- Section 17 of the DPDP Act read with Rule 15 exempts the applicability of the DPDP Act and the Draft Rules to processing of personal data, when such processing is conducted for research, archival or statistical purposes, provided that it is carried on in accordance with prescribed standards. Schedule 2 to the Draft Rules lays down the standards that must be adhered to in the course of carrying out processing for research, archival or statistical purposes which includes requirements such as, that the processing is carried out in a lawful manner, only necessary personal data must be collected and reasonable efforts should be made to ensure the accuracy of data being collected.

CONCLUSION

The Draft Rules represent an attempt at ensuring protection of personal data of individuals in India. Representatives of the MeitY have expressed that the Draft Rules aim to strike a balance between safeguarding user privacy and addressing the evolving needs of digital businesses and regulatory bodies. For businesses, particularly small and medium enterprises, compliance may require substantial investments in infrastructure, consent management systems, and data security. For users, the Draft Rules offer the possibility of enhanced privacy protections and a framework for greater autonomy over personal data that they share with organisations. However, concerns about the broad powers of government access to data, potential overreach, and the absence of adequate safeguards must be addressed to ensure a balance between privacy protection and national security interests.

Stakeholders have the opportunity to provide their comments and feedback on the Draft Rules until 18th February 2025.

*****

DISCLAIMER

MUMBAI

13th Floor, Express Towers, Ramnath Goenka Marg, Nariman Point, Mumbai – 400 021

Tel : +91 22 4241 0000

NEW DELHI

Flat No. 14(II), 2nd Floor, Front Block, Sagar Apartments, 6, Tilak Marg, New Delhi – 110 011.

Tel : +91 11 4610 2548

PUNE

2nd Floor, Kundan Chambers, Thube Park, Next to Sancheti Hospital, Pune – 411 005

Tel : +91 20 2553 0711

WWW.PARINAMLAW.COM