nota bene

UPDATE

9 January 2025

This Update has been prepared by Rajarshi Dasgupta, Subarna Saha and Muskan Madhogaria

FREQUENTLY ASKED QUESTIONS ON THE DRAFT DIGITAL PERSONAL DATA PROTECTION RULES, 2025

The much-awaited draft Digital Personal Data Protection Rules, 2025 ("**Draft DPDP Rules**") have been released which will operationalise the Digital Personal Data Protection Act, 2023 ("**DPDP Act**") enacted in August 2023 which is yet to come into force. The Ministry of Electronics and Information Technology has released the Draft DPDP Rules along with an explanatory statement on 3 January 2025 for public consultation and stakeholder comments, which can be submitted through the MyGov portal on or before 18 February 2025.

The DPDP Act provides a framework for consolidation of all matters relating to privacy in India and establishes Data Protection Board of India ("**Board**") for regulating the compliances under the DPDP Act. However, the implementation of the DPDP Act is subject to the rules as several key provisions of the DPDP Act were left to be prescribed by the central government. Hence, the Draft DPDP Rules have clarified (albeit to a limited extent), the implementation mechanism of the DPDP Act. In this issue of *nota bene,* we have endeavoured to give a bird's eye view of the compliances as per the present form of Draft DPDP Rules.

1. Who is amenable to compliances under DPDP Act and Draft DPDP Rules?

The DPDP Act and the Draft DPDP Rules are applicable to the following:

(a) *Data Principal*: Individual to whom the personal data relates and where such individual is a child, includes the parents or lawful guardian of such a child and where a person with disability, includes her lawful guardian, acting on her behalf.

(b) *Data Fiduciary*: Person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

(c) *Data Processor*: Person who processes personal data on behalf of a data fiduciary.

(d) *Consent Manager*: Person registered with the Board, who acts as a single point of contact to enable a data principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.

2. **How will the data fiduciary give notice to the data principal for obtaining consent regarding personal data?**

The data fiduciary is required to ensure that the consent provided by data principals must be free, specific, informed, unconditional, and clearly expressed through an affirmative action.

The data fiduciary has to provide a consent notice in a clear and plain language to the data principal constituting the following:

(a) *Presentation Requirement*: The notice has to be provided in a clear, standalone, and understandable format.

(b) *Fair Account of Data Processing*: The consent notice should contain the following minimum information:
- an itemised description of personal data; and
- specific purpose of, and an itemised description of the goods or services to be provided or uses to be enabled by such processing.

(c) *Information about Rights*: The consent notice should provide website and/ or application link for:
- easy withdrawal of consent (ease of doing so being comparable to that with which such consent was given);
- exercise of rights under the DPDP Act; and
- filing of complaints with the Board.

3. **What baseline security safeguards should data fiduciaries and data processors adopt to secure data principal's personal data?**

DPDP Rules prescribe the following minimum safeguards for protection of personal data under the control of data fiduciary (and data processors engaged by such data fiduciary):

(a) Security of personal data through encryption, obfuscation or masking or the use of virtual tokens mapped to that personal data;

(b) access control measures over the computer resources;

(c) maintenance, monitoring and review of access logs of personal data to enable detection of unauthorised access, its investigation and remediation to prevent recurrence;

(d) reasonable measures like data back-ups to ensure continuity in terms of confidentiality and integrity of personal data in case of destruction/ loss of access to personal data or otherwise; and

(e) To enable detection of unauthorised access, retention of prescribed logs and personal data for a period of 1 (one) year, unless compliance with any law for the time being in force requires otherwise.

4. What is the procedure to be followed by the data fiduciary in case of breach of personal data?

In event of a personal data breach, the obligation to notify data breach to both affected data principal and the Board does not have any materiality qualifier under the Draft DPDP Rules which implies that data fiduciaries will have to follow the notification requirement for all kinds of data breaches, whether big or small.

The two-step intimation requirement is as follows:

Step 1: Intimation to the Affected Data Principal: The intimation will be done without delay in a concise, clear and plain manner through data principal's user accounts including email/ mobile number/ or other means of accessing a data fiduciary's services mentioning:

- A brief description of the breach including timing and location of occurrence;
- risk mitigation measures implemented by data fiduciary; and
- contact details of designated person of data fiduciary to respond to related queries.

Step 2: Intimation to the Board: Upon becoming aware of the data breach, a 2-step notification by the data fiduciary has been prescribed:

- Initial Notification: Immediate notification containing basic information like description, nature, timing, location of breach, etc.

- Detailed Notification: To be done within 72 (seventy-two) hours (may be extended by Board basis a request in writing by data fiduciary) of becoming aware of a breach. The detailed notification must *inter alia* contain information on who caused the breach, remedial measures taken to prevent reoccurrence and report about intimations to data principals.

5. What is the timeline for retention of personal data by a data fiduciary?

The data fiduciaries of the following category:

(a) e-commerce entities having not less than 2,00,00,000 (two crore) registered users in India;
(b) online gaming intermediaries having not less than 50,00,000 (fifty lakh) registered users in India; and
(c) social media intermediaries having not less than 2,00,00,000 (two crore) registered users in India,

shall retain the personal data for a period of 3 (three) years from the date on which the data principal last approached the data fiduciary for exercising their rights or commencement of the draft DPDP Rules, whichever is the latest.

6. What steps shall data fiduciary undertake prior to data erasure?

Before erasing personal data, a data fiduciary must ensure that retention of such personal data is not necessary for compliance with any applicable laws and no data principal has approached them for the performance of the specified purpose or exercising their rights concerning the data within a period of 3 (three) years for entities mentioned in FAQ 4. In the event, both the aforementioned pre-requisites are satisfied, the data fiduciary must notify the data principal, at least 48 (forty-eight) hours before the scheduled erasure, that unless they log into their user account or otherwise initiate contact with the data fiduciary for the performance of the specified purpose or exercise their rights in relation to the processing of such personal data, their data will be erased.

7. What is the eligibility requirement for registration as a consent manager?

The data fiduciary has to be onboarded on the platform maintained by the consent manager who will facilitate consent between data principal and data fiduciary. The Draft DPDP Rules have now prescribed *inter alia* the following eligibility requirement for registration as consent manager:

(a) a company incorporated in India with sufficient financial, technical and operational capacity;

(b) company has a minimum net worth of INR 2,00,00,000 (Indian Rupees Two Crore only);

(c) the directors/ KMPs/ senior management of the company are individuals with a general reputation for fairness and record of fairness and integrity;

(d) the charter documents of the company should contain provisions to mitigate conflict of interest with data fiduciaries;

(e) the interoperable platform of the company is certified to be consistent with prescribed standards of the Board; and

(f) the company has in place technical and operational measures to display on its website/ application prescribed information regarding its shareholders and directors.

8. How can data fiduciaries obtain verifiable consent of a parent/ lawful guardian before processing the personal data of children or individuals with disabilities?

To safeguard the personal data of children and person with disabilities, the DPDP Act prescribes obtaining verifiable consent from their parents/ lawful guardians. The Draft DPDP Rules mandates data fiduciaries to adopt appropriate technical and organisational measures to verify the identity and age of a parent or lawful guardian before processing any child's personal data.

To ensure that the individual identifying herself as the parent is an adult who is identifiable by reference to:

(a) reliable details of identity and age as available with the data fiduciary; or

(b) voluntarily provided details of identity and age or a virtual token (e.g., token verified and made available by a Digital Locker) mapped to the same.

Separately, data fiduciary has to observe due diligence to verify that such guardian is appointed by a court of law, a designated authority or a local level committee, under the law applicable to guardianship.

9. What are the additional obligations for significant data fiduciaries?

Under the DPDP Act, a specific class of data fiduciaries will be designated as significant data fiduciaries basis certain prescribed conditions. These significant data fiduciaries are required to adhere to the following additional compliances beyond those imposed on general data fiduciaries:

(a) *Data Protection Impact Assessment ("**DPIA**")*: A DPIA and audit to ensure effective observance of the DPDP Act has to be conducted every 12 (twelve) months from the date when the entity is notified to be significant data fiduciary.

(b) *Reporting to the Board:* The significant data fiduciary shall cause the person undertaking the DPIA and audit to submit a report to the Board containing the key findings from these assessments.

(c) *Due Diligence:* Due diligence to be conducted to ensure that the software deployed for data hosting, display, uploading, storage, and sharing personal data, does not jeopardize the rights of data principals.

(d) *Data Localisation:* Significant data fiduciary to ensure that both the personal data and any ancillary traffic data remains within the territory of India.

10. Will all businesses be required to store personal data within India?

Only such data fiduciaries who fall under the category of significant data fiduciaries will have to store certain specified data in India. The eligibility criteria for significant data fiduciary and the specific category that will be subject to localisation, will be notified by the central government at a later date.

11. What information will a data fiduciary be required to publish on its website/ application?

The following are the publishing requirements of data fiduciaries as per the Draft DPDP Rules:

(a) business contact information of data protection officer/ any person who can answer queries of data principals on behalf of data fiduciaries regarding processing of personal data;
(b) method of making a request by data principal for the exercise of their rights;
(c) the particulars, if any, such as the username or other identifier of such a data principal, which may be required to identify them; and
(d) timeline for grievance redressal.

While the Draft DPDP Rules are a welcome step in the right direction, there still exists ambiguity and the industry will look forward to a more comprehensive and clear set of rules, once the stakeholders' recommendations are considered for finalising the rules.