January 2025

Draft Digital Personal Data Protection Rules, 2025

Background

The Digital Personal Data Protection Act, 2023 ("**DPDP Act**") was enacted in August 2023. Pursuant to this, the Ministry of Electronics and Information Technology ("**MeitY**") published the Draft Digital Personal Data Protection Rules, 2025 ("**Draft Rules**") for public consultation on 3 January 2025. MeitY has invited stakeholder comments on the Draft Rules, which may be submitted up until 18 February 2025. The Draft Rules provide guidance on operationalising various legal obligations and requirements under the DPDP Act. A summary of the key provisions under the Draft Rules are set out below.

Please note that the Draft Rules relating to commencement thereof, definitions and matters of the Data Protection Board ("**DPB**") will come into force upon publication of the final Rules in the Official Gazette. All the other Draft Rules will come into effect at a later date (yet to be specified).

Key Highlights

Notice

Data Fiduciaries are required to provide a notice to Data Principals seeking their consent prior to processing their Personal Data ("**PD**"). The Draft Rules provide further clarity on the contents of such notice. This includes (i) an itemised description of PD being processed, as well as (ii) a description of the goods or services to be provided or uses to be enabled, pursuant to such processing.

Reasonable Security Safeguards

The DPDP Act requires Data Fiduciaries to protect PD and prevent PD breaches by implementing reasonable security measures. While the Draft Rules do not prescribe compliance with any specific industry standard, they do set out minimum technical safeguards that must necessarily be undertaken. These, *inter alia*, include: (i) implementation of access control measures; (ii) maintenance and monitoring of logs of PD access; and (iii) maintenance of back-up data.

Personal Data Breach Notification

On becoming aware of any PD breach, *without any delay*, Data Fiduciaries will be required to intimate PD breaches separately to the DPB and to affected Data Principals.

Notification to DPB:

- On becoming aware of the breach, the Data Fiduciary will be required to provide to the DPB a description of the breach, including its nature, extent, timing, location of occurrence, and likely impact.
- Within 72 hours of becoming aware or such longer time as the DPB may allow upon request, the Data Fiduciaries will also need to *subsequently* provide to the DPB updates to information provided in the earlier intimation, if any, including information on findings regarding the person who caused the breach and a report regarding the intimations given to affected Data Principals.

Notification to Affected Data Principals:

- On becoming aware of the breach, the Data Fiduciary will also need to provide to the each affected Data Principal: (i) a description of the breach, including its nature, extent, timing, and location of occurrence; (ii) consequences to the Data Principal likely to arise from the breach; (iii) risk mitigation measures being/implemented; (iv) the safety measures that the Data Principal may take to protect their interests; and (v) business contact information of Data Fiduciary's authorised personnel for handling Data Principals' queries.

Since the reporting requirement is triggered when a Data Fiduciary becomes aware of a PD breach, it may need to inform multiple affected Data Principals in stages as the breach's impact becomes clearer. Similarly, it may need to keep updating the information shared with the DPB about the breach.

Processing PD Outside India

The Draft Rules provide that any entity processing PD within

India or outside India (in relation to offering goods/services to Data Principals in India) may only transfer PD to any country/ territory outside India subject to any restriction imposed by the Central Government on making such PD available to a foreign State or entities or agencies under its control.

Notably, Section 16 of the DPDP Act which governs cross-border data transfers only empowers the Central Government to restrict, through notification, the transfer of PD to a particular country or territory. The provision does not empower the Central Government to impose conditions on transfer of PD outside India, and as such, it remains to be seen how this provision in the Draft Rules will be operationalised.

Verifiable Consent Requirements for Children and Persons with Disability

Data Fiduciaries will have to undertake due diligence measures when obtaining verifiable consent from parents or lawful guardians prior to processing PD of children or persons with disability who have a lawful guardian. The consent management process for these categories of persons will, however, be different:

Children:

- Verifiable consent of the parent will have to be obtained before the processing of their PD, and
- The individual identifying themselves as the parent will have to be verified as an identifiable adult.

Persons with disability having a lawful guardian:

- The individual identifying themselves as the lawful guardian of such a person will have to be verified as having been duly appointed as such under applicable guardianship laws.

However, the Draft Rules do not provide guidance on how Data Fiduciaries will, in the first place, establish that a Data Principal is a minor or a person with disability with a lawful guardian.

Exemptions *re* Children's PD

The Draft Rules exempt certain classes of Data Fiduciaries from the verifiable consent requirement while processing PD of children and from the prohibition on tracking, targeting advertisements at, or behaviourally monitoring children, subject to certain conditions. For e.g.:

- Educational institutions are exempt where they track and behaviourally monitor children for educational activities or for safety reasons.
- Clinical establishments, mental health establishments or healthcare professionals are exempt to provide health services, necessary for protecting the child's health. Similar exemptions have been granted to allied healthcare professionals
- Individuals working in creches or child day care centres are exempt where they track and behaviourally monitor children for safety reasons.

The Draft Rules also exempt processing of PD of children for certain "purposes" from these obligations / restrictions. For e.g.:

- Processing PD of children to ensure that harmful information is not accessible by them has been exempted.
- Processing PD for creating email accounts for children, to enable them to communicate via email, has also been exempted.

Time Period for Retention of PD

According to the DPDP Act, Data Fiduciaries will need to erase PD in their control, when, *inter alia*, the "specified purpose" (that is, the purpose for processing PD as stated in the consent notice) is no longer being served. The Draft Rules clarify the timelines for determining when the "specified purpose" for processing PD will be deemed as no longer being served.

For e-commerce entities, social media intermediaries, and online gaming intermediaries, with more than 2 crores or 50 lakh registered users in India, respectively, this period has been specified as 3 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, whichever is later.

At least 48 hours prior to the expiry of the prescribed time period within which the specified purpose will be deemed to have lapsed, Data Fiduciaries will need to inform affected Data Principals that:

- Their PD will be erased due to lack of contact with the Data Fiduciary for performance of the specified purpose, or exercise of their rights; and
- That their PD will *not* be erased if, before the expiry of such a period, they log in to their user account, or otherwise initiate contact.

Ongoing Obligations of Significant Data Fiduciaries ("SDFs")

The Draft Rules prescribe certain new obligations for SDFs, such as:

Data Localisation:

- In a significant new addition, the Draft Rules require SDFs to undertake measures to ensure that they do not transfer any PD (and traffic data related to its flow) outside India as may be identified by the Central Government

upon recommendations of a "committee" it constitutes. It is notable that the DPDP Act does not envisage the constitution of any committee for imposing any restrictions on cross-border data transfers, specifically for SDFs, nor does the DPDP Act provide for any regulation of non-personal data such as traffic data (which is outside the scope of the statute).

Impact Assessments, Audits and Ongoing Due Diligence:

- The Draft Rules provide that SDFs will further need to undertake a Data Protection Impact Assessment and audit once a year and ensure that the key observations of the assessment and audit are shared with the DPB. However, the Draft Rules do not clearly distinguish between the impact assessment and audit, and what each entail. SDFs will also be required to observe due diligence to ensure that any algorithmic software that they deploy for hosting, display, uploading, etc., of PD processed by them are unlikely to risk the rights of Data Principals.

Registration and Obligations of Consent Managers

The Draft Rules elaborate on the framework of 'Consent Managers' envisaged under the DPDP Act.

- Consent Managers can register with the DPB, upon meeting specific conditions, including being an Indian incorporated company and having a certified interoperable platform for Data Principals to use that is consistent with data protection standards and assurance framework that the DPB may publish.
- Once registered, Consent Managers will need to adhere to certain obligations. Failure to do so may lead to suspension or cancellation of registration.

Power to Call for Information

Under the DPDP Act, the Central Government is empowered to seek information from a Data Fiduciary or intermediary. The Draft Rules now specify the purposes for which such information may be sought, along with the authorised person who may seek such information. For e.g.:

- For purposes related to the sovereignty and integrity of India or national security, the authorised person will be designated by the Central Government.
- For notifying a Data Fiduciary (or class thereof) as an SDF, the authorised person will be an officer attached to the MeitY, as designated by the Secretary, MeitY.

An authorised person is empowered to specify the timelines within which information has to be furnished and, where necessary, prohibit the Data Fiduciary or intermediary from further disclosing such a request.

Appointment of DPB

The Draft Rules empower the Central Government to constitute two 'Search-cum-Selection Committees' to recommend the appointment of the Chairperson and other Members of the DPB.

Appeal against Orders of DPB

Appeals against orders or directions of the DPB may be filed digitally before the Appellate Tribunal (*i.e.*, the Telecom Disputes Settlement and Appellate Tribunal). Notably, the Tribunal will not be bound by the procedure laid down by the Code of Civil Procedure, 1908 and shall be guided by the principles of natural justice instead. It will also have the power to regulate its own procedure.

Please get in touch with the SAM & Co. attorney you regularly work with if you would like to discuss any aspect of the Draft Rules in more detail.

SAM & Co. is a leader in the data protection field in India. The Firm's data privacy and cybersecurity practice specialises in issues relating to data privacy and data governance, cross border data flows, data sharing arrangements, internet and content regulation, intermediary liability, cybersecurity, and emerging technology. The Firm has also represented several clients in landmark privacy and data protection litigation before various courts in India and regularly provides legal and public policy inputs to the Government, leading foreign and Indian businesses and to trade associations.