DORSEY
DORSEY+WHITNEY LLP

India Draft Digital Personal Data Protection Rules, 2025

January 27, 2025 – The TMCA
by Charlene Krogh

MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY GOVERNMENT OF INDIA
सत्यमेव जयते

This post was written by Indian Law expert, Cyril Abrol, of the law firm Remfry & Sagar and republished with permission from Remfry & Sagar. For more information about Remfry & Sagar and their attorneys, please visit: https://www.remfry.com/.

On January 03, 2025, the government released the much awaited draft Digital Personal Data Protection Rules, 2025, (Draft Rules / Rules) for public consultation and invited stakeholder feedback by February 18, 2025 (access the Rules here).

The Rules aim to provide an operational framework for the Digital Personal Data Protection Act, 2023 (DPDP Act /Act) which was enacted on August 11, 2023, establishing a framework for protecting digital personal data by regulating its processing in India (read a synopsis here and here). It is also applicable to processing digital personal data outside India, if it involves providing goods or services to data principals (individuals to whom the personal data relates) within the territory of India.

Highlights of the Rules include:

Notice for consent

To obtain informed consent from a Data Principal, a Data Fiduciary must provide it with a clear and standalone notice outlining what data is to be collected, the purpose for the processing, and details of goods /services to be provided or uses to be enabled by the data processing. Additionally, it should contain a direct communication link through which data principals may withdraw consent, file a complaint to the Data Protection Board

Related People

- Charlene Krogh

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

('Board') etc.

Consent Managers

The DPDP Act defines a 'Consent Manager' as "*a person registered with the Board who acts as a single point of contact to enable a data principal to give, manage, review, and withdraw consent through an accessible, transparent, and interoperable platform.*"

Under the Rules, a Consent Manager must be a company incorporated in India, having a minimum net worth of INR 20 million to ensure financial stability and have a sound reputation and record of fairness, integrity and operational capacity.

Security Safeguards

Data Fiduciaries must implement measures such as encryption, obfuscation or masking of personal data, access control, monitoring of breaches and unauthorized activities as well as ensure continuity in processing. The Rules set out minimum technical safeguards that include: (i) implementation of access control measures; (ii) maintenance and monitoring of logs of PD access; and (iii) maintenance of back-up data.

Data Breach Notification

The Rules mandate that all personal data breaches must be reported to both affected users and the Board. Upon becoming aware of a breach, organisations are required to immediately notify affected individuals with comprehensive details including the breach's description, nature, extent, timing, location, potential consequences, risk mitigation and recommended safety measures and contact information for inquiries.

Similar information must be concurrently reported to the Board within 72 hours of becoming aware of the breach.

Data Retention Policies

E-commerce platforms with over 20 million registered users, online gaming intermediaries with over 5 million users and social media intermediaries with over 20 million users must delete user data after 3 years of inactivity.

Children's and Disabled Persons' Data

Data fiduciaries must implement measures to ensure that consent for a child's data is given by their parent and verification is performed to confirm that the consenting party is an adult. Consent for a disabled person is to be obtained from their legal guardian and it must be verified that the guardian has been appointed under applicable guardianship laws.

However, there is ambiguity on how it will be established that a Data Principal is a minor or a person with disability.

Further, certain Data Fiduciaries, such as healthcare providers or educational

institutions, may be exempt from specific obligations when processing children's data, under defined conditions. For instance, educational institutions are exempt where they track and behaviourally monitor children for educational activities or for safety reasons.

Also, processing of personal data for research, archival, or statistical purposes is exempt if it complies with prescribed safeguards (listed in Schedule II to the Rules).

Cross-Border Data Transfer Guidelines

Restricted /prohibited territories have not yet been notified. Data fiduciaries must ensure compliance with conditions set by the government, through general or special order, for making personal data available to foreign states or entities.

Annual Data Protection Impact Assessments (DPIAs)

If the Central Government identifies an entity as a Significant Data Fiduciary based on enumerated factors, including volume and sensitivity of the data processing, that entity must conduct annual DPIAs to assess risks associated with their data processing activities and submit their findings to the Board.

Once the Rules are finalised, the government will begin appointing members of the Board. Rules meant for businesses /industry will likely take effect in a staggered manner – one report hints at a two year sunrise period for industry to transition to the new law.