On 13 November 2025, the Ministry of Electronics and Information Technology notified the Digital Personal Data Protection Rules 2025 (Rules).

The Rules clarify key implementational aspects of the Digital Personal Data Protection Act 2023 (DPDPA), marking a significant milestone in the rollout of India's first comprehensive data protection law. A summary of the implementation timeline, key changes from the draft version of the rules previously released for public consultation, and the key provisions of the Rules are provided below.

Implementation timeline

Along with the notification of the Rules, the Government has notified a phased timeline for implementing the DPDPA as follows:

(i) **Immediately effective:** (a) definitions under the DPDPA (e.g., that of personal data, Data Fiduciary[1], etc.); (b) provisions establishing the Data Protection Board of India (Board) along with its administrative machinery; (c) the rule-making and transitional powers of the Government of India; and (d) the ability to make amendments to the DPDPA.

(ii) **After 1 year (i.e., 13 November 2026):** The conditions for registration and operation of consent managers as well as the Board's corresponding jurisdiction over being intimated of any breach of such conditions.

(iii) **After 18 months (i.e., 13 May 2027):** The core operational provisions of the DPDPA, relating to: (a) consent and corresponding aspects; (b) obligations applicable to Data Fiduciaries; (c) obligations applicable to significant Data Fiduciaries[2]; and (d) the remaining powers of the Board.

Notably, the existing data protection framework under Section 43A of the Information Technology Act 2000 (IT Act) read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 will remain in force and not be repealed until the end of the 18-month period of implementation. However, the enforcement of the DPDPA will not impact the applicability of Section 72-A of the IT Act and corresponding penalties for the wrongful disclosure of personal data of an individual, in breach of consent, or a lawful contract with such individual.

What's new: Key changes compared to the draft released for public consultation

- **"Specific" instead of "itemized"**: The notice requirement earlier required an itemized description of goods or services to be provided. The reference to the word "*itemized*" has been replaced with "specific". Given the similarity in meaning of both words, this change may be considered less significant by businesses from a practical standpoint. This provision may still be read as requiring a mapping of categories of personal data collected with the corresponding purposes of processing as well as the specific goods or services (i.e., in relation to which such data is processed).

[1] Entities determining the purpose and means of processing personal data.
[2] Entities classified on factors such as nature and volume of personal data processed.

- **Some flexibility in security safeguards**: The draft rules required Data Fiduciaries to implement appropriate data security measures "including" a range of measures such as encryption, obfuscation, masking, etc. The Rules replace the word "including" with "such as", implying that the list of measures suggested is indicative, and may depend on the nature of data being processed as well as the corresponding processing activity.

- **New retention requirement**: The final rules introduce a new requirement (Rule (8(3)), mandating all personal data, traffic data and logs generated from data processing activities to be retained at least for 1 year, even after the fulfilment of the purpose, or deletion of the user account, for purposes specified in the Seventh Schedule. The Seventh Schedule is worded broadly to include: (i) processing of personal data by government agencies in the interest of national security and sovereignty and integrity of India; (ii) performance of any function under any law in force in India; and (iii) disclosure of any information, pursuant to any law in force in India.

- **Timeline for grievance redressal**: While the draft rules did not prescribe a timeline for grievance redressal, the Rules require that grievances are resolved within a reasonable time, not exceeding ninety days, adding certainty to the duration of internal grievance resolution processes between businesses and customers.

- **Exceptions to obligations relating to children's data**: The draft version of the rules provided for certain purposes for which children's personal data could be subject to tracking or behavioral monitoring. This list has been expanded to include the determination of real-time location of a child, where such processing is restricted to tracking real-time location of a child in the interest of their safety, protection or security. Further, children's data may also be monitored or tracked to restrict certain types of services and advertisements which may pose a detrimental effect on their well-being.

Snapshot of key provisions of the Rules

NOTICE

- **Mapping data with purposes**: As highlighted above, Data Fiduciaries are required to publish a notice, providing a fair account of the details necessary to enable Data Principals (individuals, identifiable by, or in relation to personal data) to give specific and informed consent for the processing of their personal data. The notice should, at the minimum, include the following: (i) an itemised description of personal data sought to be processed; (ii) the specified purpose(s) of processing such personal data, and (iii) a specific description of the goods or services to be provided or uses to be enabled by, such processing.

- **Independent document**: The notice is to be presented and understandable *independently*, i.e., distinguishable from any other information made available by the Data Fiduciary, (e.g., contract or terms and conditions with the Data Principal).

- **Consent withdrawal mechanism**: The Data Fiduciary must provide a specific communication link for accessing its website or app (or both), along with a description of any other available means, through which Data Principals may (i) withdraw their consent (with the process being as simple as the providing of the original consent); as well as (ii) exercise their rights under the DPDPA.

INTIMATION OF PERSONAL DATA BREACH

- **Reporting to the Board**: Data Fiduciaries must report a personal data breach through tiered notification process. The initial notification to the Board must be made without undue delay upon becoming aware of a breach. A detailed notification must be made within 72 hours of the Data Fiduciary becoming aware of such breach (or such longer time that the Board may permit upon a request made in writing in this regard). Such detailed notification must provide thorough information about the events and circumstances leading to the breach, the measures taken or proposed to mitigate the risk, findings regarding the person responsible for the breach, remedial actions to prevent recurrence, and a report regarding notifications given to affected Data Principals.

- **Reporting to Data Principals**: Affected Data Principals also need to be intimated of such breach without any delay through the Data Principals' user account or any other mode of communication registered with the Data Fiduciaries. Notably, the Rules do not prescribe a specific *timeline* for reporting a personal data breach to Data Principals.

DATA PRINCIPAL RIGHTS

- **Mechanism of exercising data principal rights**: In addition to the timeframe for resolving grievances, Data Fiduciaries must publish details of how Data Principals can exercise their rights. Data Principals may designate individuals to exercise their rights under the DPDPA using the provided means and identifiers (e.g., customer identification number / enrolment ID / username). Such a nominee can exercise the Data Principal's rights in case of death or incapacity of the Data Principal.

REASONABLE SECURITY SAFEGUARDS

- **Specification of security measures**: The Rules provide requirements of what would constitute reasonable security safeguards, such as (i) technical measures (e.g., encryption, obfuscation, masking, or using virtual tokens mapped to the personal data); (ii) access controls; (iii) monitoring and logging requirements to prevent unauthorised access and maintaining the confidentiality of personal data; (iv) continuity measures to ensure the availability and integrity of personal data; as well as (v) retention of logs for breach detection for a period of 1 year or more (if required by any other law)). It seems that the intention is not to prescribe specific standards in this regard.

INTERNATIONAL DATA TRANSFERS

- **Room for possible localisation requirements**: The Government of India may issue certain restrictions which Data Fiduciaries will be required to comply with prior to sharing or transferring personal data outside India wherein such data can be made available to any foreign State or person/entity under the control of any agency of such State. Notably, Data Fiduciaries may experience challenges in reconciling this requirement with conflicting obligations under foreign laws that may mandate the disclosure or transfer of such data (situated outside India) with government agencies in third countries (e.g., under foreign surveillance laws). Significant Data Fiduciaries (Data Fiduciaries classified based on factors such as volume and sensitivity of personal data processed) may be required to restrict the transfer of both personal data as well as traffic data (pertaining to the flow of such personal data) outside India, as specified by the Central Government basis recommendations of a committee constituted by the Central Government.

CHILDREN'S PERSONAL DATA

- **Age-Gating and verifiable parental consent:** Data Fiduciaries must obtain verifiable consent from the parent (or guardian, wherever applicable) of a child (an individual who has not completed the age of 18 years) before processing such child's personal data through appropriate technical and organisational measures. Due diligence must be undertaken to ensure that the individuals identifying themselves as parents are identifiable adults. This can be achieved either through reliable identity and age details already held by the Data Fiduciary, or voluntarily provided by the individual or by using a virtual token mapped to such details, issued by authorised entities such as Digital Locker service providers (authorised intermediaries notified by the Government of India that provide Digital Locker repository facilities).

- **Verifying guardianship**: Notably, the Rules do not *specifically* mandate data fiduciaries to verify the relationship or kinship between a child and the parent providing consent. However, when obtaining verifiable consent from an individual claiming to be the lawful guardian of a person with a *disability*, a data fiduciary must exercise due diligence to verify that the guardian in question has been appointed by a court of law, a designated authority, or a local level committee, in accordance with applicable guardianship laws.

ADDITIONAL OBLIGATIONS OF SIGNIFICANT DATA FIDUCIARIES

- **Annual filings**: SDFs are required to conduct: (i) annual data protection impact assessments (DPIAs) and (ii) audits, through an independent data auditor to ensure compliance with the DPDPA. SDFs are required to cause a report to be furnished to the Board, highlighting significant findings from the DPIA and audits.

- **Algorithmic due diligence**: SDFs must undertake due diligence to ensure that any technical measures including the algorithmic software used for handling personal data are designed and verified to safeguard against any risks to the rights of Data Principals.

SPECIFIED RETENTION PERIODS FOR CLASSES OF DATA FIDUCIARIES

- **Limitation on retention periods**: Apart from the retention requirement introduced through the Rules highlighted above, for certain classes of Data Fiduciaries, the Rules set out a maximum retention period of 3 years for personal data, starting from the later of the Data Principals' last request (whether for the performance of the specified purpose for which personal data was collected, or for exercising any of their rights under the DPDPA) or the commencement of the Rules. These classes include (i) e-commerce entities and (ii) social media intermediaries - both with 20 million or more registered users in India, as well as (ii) online gaming intermediaries with 5 million or more registered users in India. Data Fiduciaries must inform the Data Principal 48 hours prior to deleting the personal data of such Data Principal who does not initiate contact with the Data Fiduciary for the performance of the specified purpose.

CONSENT MANAGERS

- **Function of consent management:** Consent managers must enable Data Principals, using the consent manager's platform, to provide consent on their behalf. Such consent may be provided through the consent manager either *directly* to a Data Fiduciary, or *indirectly*, through another Data Fiduciary onboarded onto such platform acting as an intermediary. Significantly, this may enable Data Principals to provide consent to the processing of their personal data *interoperably*, without sharing a pre-existing interface or direct contractual relationship with every Data Fiduciary. Consent managers are required to be "data-blind" so that they are unable to read the contents of the personal data exchanged through their platform.

- **Fiduciary duty:** Consent managers are required to act in a fiduciary capacity towards the Data Principal and avoid any conflict of interest with Data Fiduciaries. Such conflict of interest may be in respect of its directors, key managerial personnel and senior management holding a directorship, financial interest, employment or beneficial ownership in Data Fiduciaries, or sharing a material pecuniary relationship with such Data Fiduciary.

EXEMPTIONS

- **Education, healthcare and child services**: The Rules exempt clinical establishments and healthcare professionals, educational institutions, creche and childcare facilities from restrictions under the DPDPA against behavioural monitoring or tracking of children for certain purposes. These include providing healthcare services, for educational activities and child safety, respectively. Notably, the Rules define educational institutions as institutions of learning, that impart education, including vocational learning. This definition leaves open the question of whether it would extend to include ed-tech companies.

- **Research, archiving or statistical purposes**: The DPDPA read with the Rules exempts the processing of personal data processed for research, archiving or statistical purposes if: (i) processing is *lawful* and *limited* to *such* purposes; (ii) data collected is *necessary* for *such* purposes; (iii) *reasonable efforts* are made to ensure *completeness, consistency and accuracy* of the data processed; (iv) data is retained *only* for as long as *required*; (v) appropriate measures are in place to prevent a personal data breach; and (vi) where applicable, contact details and a communication link are provided for Data Principals to exercise their rights. The Data Fiduciary is accountable for compliance with these conditions.

CALL FOR INFORMATION

- **Government access request**: Notably, the Rules empower the Central Government to, through authorised personnel, require a Data Fiduciary or intermediary (e.g., online service providers) to furnish personal data of a Data Principal in the interest of India's sovereignty, integrity, and security, or for performing any function under any Indian law. Except with the permission of authorised personnel, the Rules also prohibit the disclosure of such data access requests if it could jeopardise India's sovereignty, integrity, or security.

DATA PROTECTION BOARD OF INDIA

- **Condition for appointments**: The Rules, *inter alia*, lay down the terms and conditions of service of members and the chairperson of the Board, as well as their salaries and allowances. The Rules also lay down the terms and conditions of appointment and service of officers and employees of the Board.

- **Digital office**: Notably, the Board is to function as a digital office and may adopt techno-legal measures to conduct proceedings in a manner that does not require physical presence of any individual.

Comments

The notification of the Rules signifies the final leg of operationalizing India's first dedicated data protection legislation. For further clarity, the Government is also expected to notify certain additional key aspects pertaining to the law. This includes any potential restrictions on international data transfers, as well as the classification of certain entities as Significant Data Fiduciaries, which will be important for organisations to determine if additional responsibilities are applicable to them. The Rules meticulously balance regulatory certainty (through prescriptive requirements) with operational flexibility for businesses to foster innovation. As this law runs its last mile of implementation, businesses are expected to catch up, rethink existing design, practices and documentation – to materialise a compliance posture which is not only robust but also resilient.

- *Supratim Chakraborty (Partner); Harsh Walia (Partner); Abhinav Chandan (Partner); Shobhit Chandra (Counsel); Sumantra Bose (Counsel) and Siddharth Sonkar (Senior Associate)*

About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1300+ legal professionals, including 300+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit **www.khaitanco.com**