Draft Digital Personal Data Protection Rules, 2025

Key Highlights

04 January 2025

Introduction

On 3 January 2025, the Ministry of Electronics and Information Technology published a draft of the Digital Personal Data Protection Rules, 2025 (Rules) for public consultation. The consultation window closes on 18 February 2025.

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, representing a transformative shift in the nation's data protection landscape.

The Data Protection Board of India (Board), the enforcement body under the DPDPA, will be constituted upon the notification of these Rules in the Official Gazette following public consultation. The remaining provisions will come into effect at a later stage, on such dates that are specified in the final version of the Rules.

Notice

- **Itemised Description**: Data Fiduciaries (entities determining the purpose and means of processing personal data) 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) an itemised 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).

- **Communication Link**: 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 original consent provision); (ii) exercise their rights under the DPDPA; and (iii) make a complaint to the Board.

Intimation of Personal Data Breach

- **Reporting to the Board**: Data Fiduciaries must report a personal data breach to the Board without delay, and to this end, provide a description of the breach, including its nature, extent, timing, location of occurrence as well as likely impact. Further, within 72 hours of becoming aware of such breach (or such longer time that the Board may permit upon request), Data Fiduciaries are required to provide further information including (i) broad facts related to the events, circumstances and reasons leading to the breach; (ii) risk proposed or implemented risk mitigating measures; (iii) findings regarding the person

responsible for causing the breach; (iv) remedial measures to prevent recurrence, and (iv) a report regarding notifications given to affected Data Principals.

- **Reporting to Data Principals**: Affected Data Principals must also be intimated of such breach by the Data Fiduciary to the *best of its knowledge*, and without any delay, through the Data Principals' user account or any other registered mode of communication. Notably, while the Rules require that there is no delay in reporting to Data Principals, the Rules do not prescribe a specific *timeline* for such reporting.

Data Principal Rights

- **Mechanism of Exercising Data Principal Rights**: To enable Data Principals to exercise their rights under the DPDPA, Data Fiduciaries and, where applicable, consent managers must publish details of how Data Principals can exercise their rights. Notably, Data Fiduciaries and consent managers are required to disclose the response time that they will take to respond to grievances of Data Principals. This provides some discretion to Data Fiduciaries in determining the timeframe for responding to such requests. Data Principals may designate individuals to exercise their rights under the DPDPA (e.g., request erasure of their personal data) using the provided means and identifiers (e.g., customer identification file number/enrolment ID / username), particularly in the event of their death or incapacity.

Reasonable Security Safeguards

- **Specification of Baseline Requirements**: The Rules provide *baseline* requirements of what would constitute reasonable security safeguards, including (i) technical measures (such as 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. Notably, these remain baseline requirements, and Data Fiduciaries may be required to implement appropriate security safeguards *in addition to* these requirements commensurate with their nature and volume of their data processing activities. It seems that the intention is not to prescribe specific standards (like ISO) as long as the prescribed baseline requirements are met.

International Data Transfers

- **Room for Possible Localisation Requirements**: The Government of India may notify certain requirements or conditions which Data Fiduciaries will be required to comply with prior to sharing or transferring personal data (processed either within India or outside India, in connection with offering goods or services in India) with foreign states, entities, or their agencies. 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 (SDFs) (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) and a person with disabilities before processing such individual's personal data through appropriate technical and organisational measures. Due diligence must be undertaken to ensure that the individual identifying themselves as the parent is an identifiable adult. This can be achieved either through reliable identity and age details already held by the Data Fiduciary, or by using a virtual token mapped to such data 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 the algorithmic software used by them for handling personal data is designed and verified to safeguard against any risks to the rights of Data Principals.

Specified retention periods for certain Data Fiduciaries

- **Limitation on Retention Periods**: 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 2 crore or more registered users in India, as well as (iii) online gaming intermediaries with 50 lakh or more registered users in India. These retention periods, however, may not apply for certain purposes, such as (i) enabling the Data Principal to access his or her account, or (ii) access any virtual token that may be used to avail money, goods or services. 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 or the exercise of his or her rights).

Consent Managers

- **Function of Consent Management:** Consent managers must enable Data Principals, using the consent manager's platform, to provide consent to the processing of their personal data 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 contractual relationship with a Data Fiduciary. Consent managers are required to be "data-blind" so that they are unable to read the contents of the personal data exchanged interoperably 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.

- **Operational and Financial Conditions:** Consent managers must be *Indian-incorporated* companies, excluding foreign companies from being prospective applicants. The Rules set financial conditions, including a minimum net worth of INR 2 crore (approximately USD 240,000), and require the company's directors, key managerial personnel, and senior management to have a reputation for fairness and integrity. Consent managers are required to maintain a website or app through which the Data Principal can access their services. Consent managers are not permitted to sub-contract or assign the performance of any of its obligations under the DPDPA or the Rules, or transfer control of their company without the previous approval, and fulfilment of such conditions that are laid down by the Board.

- **Transparency Requirements**: Consent managers must disclose key information about their company, including (i) details of their promoters, directors, key managerial personnel and senior management; (ii) any individual who holds more than 2% of the shareholding in the company registered as consent manager; or (iii) body corporates in which any promoter, director, key managerial personnel or senior management of the company registered as consent manager holds more than 2% of shareholding.

- **Record Maintenance**: Consent managers must maintain a digital record of requests of (i) consents given, denied or withdrawn by Data Principals; (ii) notices preceding or accompanying consent requests; and (iii) instances of personal data of Data Principals shared with a Data Fiduciary.

- **Auditable Records**: Consent managers must implement effective audit mechanisms and report such audits to the Board periodically and on such other occasions as the Board may direct, in respect of their (i) technical and organisational controls, systems, procedures, and safeguards; (ii) ongoing compliance with the conditions of registration; and (iii) adherence to obligations under the DPDPA and the Rules.

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, such as 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**: Personal data may be 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 *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, through authorised personnel, to 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 requests if it could jeopardise India's sovereignty, integrity, or security, requiring the maintenance of confidentiality in relation to such requests.

Data Protection Board of India

- **Condition for Appointments**: The Rules lay down the conditions as well as 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.

- **Functional Independence**: Towards ensuring its independence, members of the Board are required to avoid a conflict of interest (financial or otherwise) which may affect the performance of their functions. 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 Rules aim to provide clarity on several critical aspects and once published in the final form, will catalyse the implementation of India's first comprehensive data protection legislation. The public consultation window presents a much-needed opportunity for all stakeholders to provide feedback and will aid in ensuring that practical pitfalls can be suitably addressed once the law is set into motion.

- Privacy & Data Protection Team

About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1200 legal professionals, including 270+ 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**