Regulatory Alert

Shardul Amarchand Mangaldas
A DECADE YOUNG, A CENTURY STRONG

November 2025

Enforcement of the DPDP Act and Notification of the DPDP Rules

On 14 November 2025, the Ministry of Electronics and Information Technology ("**MeitY**") published various notifications in the Official Gazette – which bring into force the Digital Personal Data Protection Act, 2023 ("**DPDP Act**"), the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**") (both with staggered timelines for implementation), and establish the Data Protection Board ("**DPB**") in the National Capital Region of India with four members.

Enforcement Timelines

The MeitY has notified three sets of dates (i.e., **14 November 2025, 14 November 2026, and 14 May 2027**) for the enforcement of provisions of the DPDP Act, along with corresponding provisions under the DPDP Rules. The substantive provisions of the DPDP Act and DPDP Rules come into force in 18 months, *i.e.*, 14 May 2027. Please refer to the Annexure for more details on enforcement timelines.

While the substance of the DPDP Rules remains largely the same as that of the Draft Digital Personal Data Protection Rules, 2025 which were released for public consultation earlier this year ("**Draft Rules**"), there are a few notable changes. The other changes are minor including consistency and language changes.

Set out below is a summary of some of the notable changes from the Draft Rules.

Key Highlights of DPDP Rules

Definitions

The DPDP Rules have a separate section on 'definitions' for specific terms used, but which have not been defined under the DPDP Act. None of the definitions, however, are new; they existed in the Draft Rules and now have just been placed in a definition section. That said, other key terms continue to be defined in the body of the DPDP Rules.

Reasonable Security Safeguards

The DPDP Rules stipulate minimum technical safeguards that must necessarily be undertaken. While there is no material change to these requirements from the Draft Rules, the DPDP Rules now clarify that a few of these technical safeguards would become relevant only "wherever applicable". For e.g., Data Fiduciaries ("**DFs**") have to incorporate appropriate language in contracts entered into with Data Processors for taking reasonable security safeguards only *where applicable*. This addition may particularly benefit smaller entities in operationalizing reasonable security practices.

Reporting of Personal Data ("PD") Breaches

As with the Draft Rules, the DPDP Rules prescribe a two-tier reporting requirement to the DPB, as well as reporting to all affected Data Principals, regardless of the impact or materiality of a PD breach. While there is no material change to these requirements from the Draft Rules, the DPDP Rules clarify that the *location* of a breach need not be disclosed to affected Data Principals.

Time Period for Retention of PD

As per the DPDP Act, DFs need to erase PD when, *inter alia*, the "specified purpose" (i.e., the purpose for processing PD as stated in the consent notice) is no longer being served. The DPDP Rules provide timelines for e-commerce entities, social media intermediaries, and online gaming intermediaries, each with users above a specific threshold, for erasure of PD.

For these entities, PD must be erased except: (a) if retention is necessary for compliance with applicable law, **or** (b) if, for the relevant time period specified in the Third Schedule, the Data Principal neither approaches such DF for the performance of the specified purpose nor exercises her rights in relation to such processing. The insertion of "or" is new under the DPDP Rules. Apart from this, there is no material change in the retention obligation for such entities.

That said, all DFs now also have to retain PD, associated traffic data, and other logs of processing such PD (whether processed by them or a Data Processor), for at least one year from the date of such processing. Such retention is for the purposes specified in the Seventh Schedule to the DPDP Rules. **This is an additional data retention obligation that was not present under the Draft Rules.**

Right to Grievance Redressal

The DPDP Rules require DFs and Consent Managers to resolve grievances of Data Principals within a reasonable period, but **no later than ninety days**. This is a change from the Draft Rules, which had earlier granted DFs / Consent Managers the flexibility to determine the time period within which they would resolve grievances.

Verifiable Consent Requirements *re* Children

The operational aspects of obtaining verifiable consent of parents or lawful guardians prior to processing PD of children are provided under the DPDP Rules. As part of this, the individual identifying themselves as the parent should be verified as an identifiable adult and the process of carrying out such verification has been stipulated.

One of the ways in which such verification can take place is *via* a virtual token mapped to details of age and identity, as issued by an "authorised entity". The Draft Rules had earlier envisaged such authorised entity as one which is entrusted by law or the Government with the *maintenance* of details regarding age and identity. The DPDP Rules, on the other hand, define authorised entity as one that deals with the *issuance* of such details (or virtual tokens mapped to the same). **The practical impact of this change (if any) may need to be further analysed.**

Exemptions *re* Processing Children's PD

As with the Draft Rules, the DPDP Rules continue to exempt certain classes of DFs from the verifiable consent requirement while processing PD of children and from the prohibition on tracking, targeting advertisements at, or behaviourally monitoring children. The DPDP Rules also exempt certain "purposes" from these obligations / restrictions. **The DPDP Rules have additionally included tracking the real-time location of a child for her safety as an exempted purpose.**

Verifiable Consent Requirements *re* Persons with Disabilities ("PWDs")

The operational aspects of obtaining verifiable consent from lawful guardians of PWDs have been provided under the DPDP Rules and a separate rule has now been carved out for this purpose. Notably, the definition of "PWDs" has been updated in the DPDP Rules. It includes individuals with autism, cerebral palsy, intellectual disability, or multiple severe disabilities who *cannot*, even with proper support, make legally binding decisions. **This nuance was lacking in the Draft Rules.**

Obligations of Significant DFs ("SDFs")

The DPDP Rules prescribe additional obligations for SDFs. This includes the requirement for SDFs to undertake measures to ensure that they do not transfer PD (and traffic data related to its flow) outside India, as may be identified by the Central Government upon the recommendation of a "committee". **The DPDP Rules now prescribe the constitution of such a committee**, *i.e.*, it will include officials from MeitY and may also include officials from other Ministries or Departments of the Central Government.

In addition, the DPDP Rules require every SDF to undertake due diligence measures to verify that its technical measures, including algorithmic software, do not pose a risk to the rights of Data Principals. This widens the scope from the Draft Rules, which required verification of just algorithmic software.

Power to Call for Information

The DPDP Rules, read with the Seventh Schedule, specify the purposes for which information may be sought from DFs or intermediaries, along with the authorised person who may seek such information. Earlier, the Draft Rules linked this information sharing obligation to Section 36 of the DPDP Act (on the power of the Central Government to call for information). While the scope of obligations to produce information remains the same, **the reference to Section 36 has been deleted from the DPDP Rules.**

Annexure

Enforcement Timelines – DPDP Act and the DPDP Rules

As noted above, the DPDP Act and the DPDP Rules are being enforced in a phased manner. The table below provides an indicative list of provisions that will take effect, as per the following staggered timelines.

Sr. No.	Date of Enforcement	Indicative Provisions Taking Effect
1.	Immediate, i.e., November 14, 2025	• Commencement provisions of the DPDP Act and DPDP Rules • Establishment of the DPB • Amendments to the Right to Information Act, 2005 and the Telecom Regulatory Authority of India Act, 1997
2.	12 months from the date of publication of the DPDP Rules and the notification enforcing the DPDP Act, i.e., November 14, 2026	• Registration of Consent Managers • DPB's powers to inquire into a breach of conditions of registration of Consent Managers and to impose penalties
3.	18 months from the date of publication of the DPDP Rules and the notification enforcing the DPDP Act, i.e., May 14, 2027	• Notice and consent requirements • Reporting of PD breaches • Implementation of reasonable security safeguards • Verifiable consent requirements for children's PD and PD of PWDs • Obligations of SDFs • Rights of Data Principals • Cross-border transfer of PD • Powers and functions of the DPB • Repeal of Section 43A of the Information Technology Act, 2000

Please get in touch with Shahana Chatterji (shahana.chatterji@amsshardul.com), Kirti Mahapatra (kirti.mahapatra@amsshardul.com), or any other attorney at SAM & Co. that you regularly work with if you would like to discuss any aspect of the DPDP Act or DPDP Rules in more detail.

SAM Co. is a leader in the data protection field in India. The Firm's data privacy and cyber-security practice specialises in issues relating to data privacy and data governance, cross-border data flows, data sharing arrangements, internet and content regulation, intermediary liability, cyber-security, 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 Indian Government, leading foreign and Indian businesses, and trade associations.