Digital Personal Data Protection Act and Rules come into effect: What you need to know?

The Ministry of Electronics and Information Technology, through its notification dated 13 November 2025, has brought the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**") into effect in a staggered manner. Read together with the Digital Personal Data Protection Act, 2023 ("**DPDP Act**"), which received Presidential assent on 11 August 2023, only certain provisions of the DPDP Rules and DPDP Act have presently come into force, marking an important step towards establishing a comprehensive framework for Digital Personal Data[i] protection and processing in India.

We have hereinbelow bifurcated the data protection framework introduced by the DPDP Act and DPDP Rules in three parts on the basis of their enforcement timelines:

A. Phase 1[ii] - Primarily dealing with the foundational clauses governing scope, interpretative framework and the institutional apparatus brought into force from 13 November 2025;
B. Phase 2[iii] - Operationalisation of the consent management framework with effect from 13 November 2026; and
C. Phase 3[iv] - Complete operationalisation of the data protection framework from 13 May 2027.

1. Understanding what Phase 1 entails

The provisions currently in enforce pertain to (i) applicability and commencement, (ii) definitions, (iii) establishment of the Data Protection Board of India ("**Board**"); (iv) protection to government and Board for actions taken in good faith, (v) miscellaneous provisions such as, bar on jurisdiction, supersession of the DPDP Act over other laws governing the subject matter, etc; (vi) amendments to Telecom Regulatory Authority of India Act, 1997 ("**TRAI Act**") and Right to Information Act, 2005 ("**RTI Act**").

The phased commencement of these provisions signals that the Government has begun laying the statutory pathway for safeguarding the digital Personal Data of individuals by operationalising the regulatory and adjudicatory structure envisaged under the DPDP Act. This is a welcome development as India has long been positioned as a global back-office hub for data processing, yet the absence of a comprehensive, accountability-driven legal framework had weakened that reputation. This led several jurisdictions to reconsider locating data-processing functions in India. The present rollout is expected to reinforce confidence in India's data-governance regime and strengthen its standing as a trusted processing destination.

The Government is presently in the process of constituting the Board, comprising a Chairperson and such other Members as may be notified, with the intention of completing the appointment process by December 2025[v]. Upon its establishment, the Board shall, to the extent practicable, function as a digital office and adopt appropriate techno-legal measures for Personal Data breaches and compliance enforcement under the DPDP Act.

Additionally, the amendments to the TRAI Act and RTI Act have now been enforced which means (i) the appellate authority under the DPDP Act will be Telecom Disputes Settlement and Appellate Tribunal set up under the TRAI Act and (ii) personal information is now explicitly exempted from being disclosed in response to right to information applications filed under the RTI Act.

2. Understanding what Phase 2 entails[vi]

The provisions to be enforced on 13 November 2026 pertain to the registration and operationalisation of Consent Managers[vii]. To qualify for registration as a Consent Manager, a person must inter alia be an Indian incorporated company with adequate technical, operational, and financial capacity to discharge its obligations. Its financial position, and governance standards must be sound, and it must have a minimum net worth of ₹20 million[viii]. The company's directors, key managerial personnel, and senior management must possess a reputation for fairness and integrity. Its constitutional documents must mandate adherence to the obligations for avoiding conflict of interest with Data Fiduciaries[ix].

As part of its obligations[x], the Consent Manager must enable Data Principals to give, manage, route, and withdraw consent through its platform, while ensuring that any Personal Data shared is not readable by it. Consent Managers are required to maintain detailed records of consents, notices, and data sharing for at least seven years and provide Data Principals access to such records in machine readable form. Amongst other requirements, the Consent Manager must operate through its own website or app, avoid conflicts of interest, act in a fiduciary capacity, and implement reasonable security safeguards. Additionally, Consent Managers, must also publish specified ownership and governance information, maintain effective audit mechanisms, and obtain prior Board approval before any transfer of control.

However, there appear to still be significant gaps in the eligibility framework for Consent Managers, as key requirements such as appropriate technical and organisational measures, independent certification of interoperability, sufficiency of technical, operational and financial capacity, and what will be the requirements for adequacy of business volume remain undefined. These open ended standards echo the DPDP Act's reliance on the phrase "*as may be prescribed*".

3. Understanding what Phase 3 entails

The said phase will essentially operationalise the entire gamut of the data protection framework in India. As has been notified by the DPDP Rules when read with DPDP Act, the key provisions of the law are as follows:

a) Comprehensive Notice and consent obligations under the DPDP Act and DPDP Rules[xi]

A Data Fiduciary must ensure that any request for consent is accompanied or preceded by a notice (*in English or in any language listed in the Eighth Schedule to the Constitution of India*) which is independently understandable, written in clear and plain language, and provides a fair and itemised account of the categories of Personal Data proposed to be processed and the specific purposes or goods or services for which such processing is sought. The notice must precede or accompany the consent request and should clearly set out the manner in which the Data Principal may withdraw consent, exercise her rights, and seek grievance redressal, together with the specific communication link to access the relevant website or app for these actions, and must also explain how a complaint may be made to the Board. Where consent was obtained prior to the commencement of the Act, this notice must still be issued immediately however, the Data Fiduciary may continue to process the Personal Data until and unless the Data Principal withdraws her consent. The notice shall be either in English or in any language listed in the Eighth Schedule to the Constitution of India. The provisions for consent largely continue to be governed by the DPDP Act[xii] with no significant supplemental provisions being introduced separately under the DPDP Rules. The essentials of the same were outlined in our previous note accessible at click here.

b) Security safeguards to protect Personal Data[xiii]

The DPDP Rules require every Data Fiduciary to implement reasonable security safeguards to protect Personal Data in its possession or control, including data handled by the Data Processors for the Data Fiduciary. These safeguards must include technical measures such as encryption, masking or tokenisation, access-control mechanisms, logging and monitoring to detect unauthorised access, data-backup and continuity measures, one-year retention of logs for investigation and remediation, contractual obligations on processors to adopt equivalent safeguards, and overarching technical and organisational controls to ensure effective compliance.

A key concern, however, is that the obligation remains framed around broad standards "*reasonable safeguards"* and "*appropriate measures*" without specifying objective technical benchmarks or certification pathways as are identified under the IT Rules of 2011. This open-ended approach may result in uncertainty, particularly for smaller organisations or those operating cross-border. As a result, while the rule outlines core security expectations, its practical contours will ultimately depend on future guidance and sector-specific standards.

c) Cross-border data transfers[xiv]

The DPDP Act and DPDP Rules leave cross-border data transfers generally permissible but subject them to any requirements that the Central Government may impose on the Data Fiduciaries for making Personal Data available to a foreign State. At present, no such restrictions have been notified, and the DPDP Rules do not elaborate further on this aspect. A negative list is therefore awaited. In our view, restrictions on cross-border transfer of data to land bordering countries similar to those prescribed for foreign investments are likely to be implemented.

d) Verifiable consent for data of Child and Disabled Persons[xv]

Under the DPDP Act and DPDP Rules, Data Fiduciaries must implement appropriate technical and organisational safeguards to ensure that a parent's verifiable consent is obtained prior to processing a child's Personal Data. They are further required to exercise due diligence to confirm that the individual providing such consent is indeed an adult identifiable by verifying identity and age from the data available with the Data Fiduciary or provided voluntarily. Likewise, when verifiable consent is sought from a person claiming to be the lawful guardian of an individual with a disability, it is the obligation of the Data Fiduciary to verify through reasonable due diligence that the guardian has been duly appointed by a court, designated authority, or local-level committee in accordance with the relevant guardianship laws.

e) Processing digital personal data for research, archiving or statistical purposes[xvi]

The DPDP Act and DPDP Rules exempt the processing of Personal Data for research, archiving, or statistical purposes, provided it is not to be used to take any decision specific to a Data Principal and where the processing is undertaken in a lawful manner in accordance with the prescribed standards namely, limiting the processing to only necessary personal data, retention is for specified timelines, appropriate technical and organisational safeguards, by following reasonable security safeguards. However, an intimation for processing should be provided to the Data Principal along with providing details of a suitable person who can address any queries.

f) Personal Data Breach and Intimation[xvii]

A Data Fiduciary must promptly notify affected Data Principals of a Personal Data breach in clear, simple terms, explaining the breach and when, there arelikely consequences on the Data Principal, steps taken to mitigate the risk, actions the Data Principal can take to protect her interest, and providing a contact person for addressing queries. It must also notify the Board without delay and, thereafter within seventy two hours, provide detailed updates on the breach, its causes, mitigation and remedial measures, and confirmation that affected Data Principals have been informed.

4. Conclusion

Overall, the staggered rollout reflects a deliberate legislative approach, first putting in place the institutional and definitional spine of the law, then activating the consent-management machinery, and finally bringing the full set of operational obligations into force. With the framework now taking shape, the direction is clear: India is moving towards a more coherent, rights-centred and accountability-driven data-protection regime. As the remaining phases become effective, organisations handling Personal Data will need to re-examine their internal policies, security practices, retention protocols and cross-border transfer arrangements to ensure they align with the new statutory standards. The transition will require sustained effort, but it is expected to bring much-needed clarity, stability and trust to India's data-governance landscape.

5. What persons[xviii] processing digital Personal Data and information should do to actively utilise the eighteen month gestation period

a) Undertake a structured assessment of all personal data currently processed and map processing activities to determine the capacity in which the organisation functions as a Data Fiduciary.
b) Clearly identify and document the purposes for which personal data is collected and processed, ensuring that such purposes bear a rational nexus with the goods or services offered and identify whether the same qualify as legitimate uses prescribed under the DPDP Act.
c) For internal governance identify and designate and equip an appropriate individual for the role of acting as a compliance lead/data protection officer or equivalent for overseeing compliance with the DPDP Act and DPDP Rules.
d) Update or formulate internal policies, data-handling practices, vendor contracts and data-processing agreements to align with upcoming statutory requirements.
e) Begin organization - wide training and sensitisation to familiarise employees, vendors and business units with the framework of the DPDP Act and DPDP Rules.
f) Start preparing notice and consent architecture, including planning for integration with Consent Managers and ensuring ease of withdrawal of consent.
g) Technical readiness to implement appropriate security and other safeguards for processing data and preparing essential systems for routing, recording, and managing consents.
h) Continuously monitor Government notifications and advisory updates, particularly as Phase II is expected to clarify standards, certification requirements, measures and prescribed safeguards.

DISCLAIMER:

This note has been written for the general interest of our clients and professional colleagues and is subject to change. This note is not to be construed as any form of solicitation. It is not intended to be exhaustive or a substitute for legal advice. We cannot assume legal liability for any errors or omissions. Specific advice must be sought before taking any action pursuant to this note. For further clarification and details or advice on the above, you may write to our Senior Partner, Ms. Statira Ranina at sranina@almtlegal.com, Associate Partner, Ms. Sheetal Mishra at smishra@almtlegal.com and Associate, Mr. Faizan Khatri at fkhatri@almtlegal.com.

******

[i] "Personal Data" means any data about an individual who is identifiable by or in relation to such data;

[ii] Section 1, 2, 18 to 26, 35, 38 to 43, 44(1) and 44(3) and Rules 1, 2, 17 and 21.

[iii] Section 6(9) and 27(1)(d) and Rule 4.

[iv] Section 3, 4, 5, 6(1) to 6(2), 6(10), 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17 and 27 except 27(1)(d), 28, 29, 30, 31, 32, 33, 34, 36, 37, and 44(2) and Rules 3, 5 to 16, 22 and 23.

[v] https://m.economictimes.com/tech/technology/search-panel-for-data-protection-board-by-december/amp_articleshow/125419136.cms

[vi] Section 6 and 27 of DPDP Act and Rule 4 of DPDP Rules.

[vii] "Consent Manager" means 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 her consent through an accessible, transparent and interoperable platform.

[viii] Part A of First Schedule of DPDP Rules.

[ix] "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

[x] Section 6 of DPDP Act, Rule 4 of DPDP Rules and First Schedule.

[xi] Section 5 of the DPDP Act and Rule 3 of the DPDP Rules.

[xii] Section 6 of DPDP Act.

[xiii] Section 8 of DPDP Act and Rule 6 of DPDP Rules.

[xiv] Section 16 of DPDP Act and Rule 15 of DPDP Rules.

[xv] Section 9 of DPDP Act and Rule 10 and 11 of DPDP Rules

[xvi] Section 17 of DPDP Act and Rule 16 of DPDP Rules.

[xviii] "person" includes (*i*) an individual; (*ii*) a Hindu undivided family; (*iii*) a company; (*iv*) a firm; (*v*) an association of persons or a body of individuals, whether incorporated or not; (*vi*) the State; and (*vii*) every artificial juristic person, not falling within any of the preceding sub-clauses.