WADHWA LAW OFFICES

Note On The Digital Personal Data Protection Rules, 2025

1. *Introduction and Background*

The Government of India notified the Digital Personal Data Protection Rules, 2025 ("DPDP Rules") on November 13, 2025, thereby formalizing India's data protection regime contained in the Digital Personal Data Protection Act, 2023 ("DPDP Act") which was notified earlier on August 11, 2023. In addition to the notification of the DPDP Rules, a series of notifications have also been issued setting out commencement dates of provisions of the DPDP Act and the DPDP Rules as well as the establishment of the Data Protection Board of India ("DPB") and its constitution. The DPDP Act and the DPDP Rules set out the framework for processing of all types of digital personal data and will apply to all organisations who process personal data in India or of persons from India.

The DPDP Rules include key operational rules for data fiduciaries (*i.e., entities that determine the purpose and means of processing, and are similar to data controllers under the GDPR*) ("Data Fiduciary") whilst also addressing the rights of data principals (*individuals to whom the personal data relates, being the data subjects under the GDPR*) ("Data Principal").

The DPDP Act and the DPDP Rules have been notified in a staggered manner with organisations being provided time to comply.

2. *DPDP Rules Implementation Timeline*

Timeline	Effective Date	Provisions Coming into Force
Immediately	**November 13, 2025**	Establishment of the DPB; digital office and inquiry procedures; rule-making powers; terms of service for DPB members.
Within 12 Months	**November 13, 2026**	Consent manager related provisions, such as registration eligibility (*Indian incorporation, minimum net worth, technical and financial capacity, governance integrity*); conflict-of-interest controls; publication of ownership/management details; 7 (seven) year consent record retention.
Within 18 Months	**May 13, 2027**	Substantive operational provisions, such as consent and notice obligations, breach reporting, security safeguards, grievance redressal timelines, Significant Data Fiduciary ("SDF") obligations, data processor controls, and retention requirements.

3. *Applicability*

The DPDP Act and DPDP Rules apply to: **(a)** any personal data processed in India; or **(b)** any personal data of Data Principals in India, processed outside India in connection with any activity which relates to offering goods or services to Data Principals in India.

The definition of '**processing**' under the DPDP Act is quite wide and is inclusive in nature, and covers within its scope, collection, storage, use, sharing, transfers of personal data, amongst other activities.

4. *Certain Exemptions*

The DPDP Rules provide limited exemptions. These include, processing of data necessary to undertake research, or for archiving or statistical purposes, provided strict safeguards are met, viz., processing must be lawful, purpose-limited, not used to make decisions about identifiable individuals, and supported by appropriate governance, accuracy, retention, and security controls.

The DPDP Rules also permit both public and private healthcare providers and educational institutions, as well as childcare settings (*i.e., an individual in whose care infants and children in a crèche or child day care centre are entrusted*), without requiring parental consent, to process personal data of children and track or target children, only for specified purposes like health services, education, safety, or preventing harmful content. New permitted purposes include determining real-time location of children and limited monitoring to ensure services or advertising are not detrimental to a child's well-being. These are purpose-specific carve-outs, requiring Data Fiduciaries to satisfy both the class and purpose conditions before relying on them.

5. *Overlap with SPDI Rules*

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 ("SPDI Rules") will remain in force for the time being, and not be repealed until the end of the 18 (eighteen) month period of implementation of the DPDP Rules, i.e., 13 May, 2027.

Until May 13, 2027, Data Fiduciaries remain accountable under: **(a)** Section 43A of the IT Act (*compensation for negligence in handling personal data*); and **(b)** the *SPDI Rules (security policies, consent for sensitive data, privacy policy)*.

This intermediate period until May 13, 2027, means: **(a)** Policies, standards, notices, and consents must remain SPDI Rules compliant; **(b)** DPDP framework aligned documentation must be prepared in parallel; and **(c)** Security frameworks must satisfy standards stipulated by the IT SPDI Rules.

From May 13, 2027, Section 43A of the IT Act, along with the SPDI Rules, will stand repealed and will be replaced entirely with the DPDP Act and DPDP Rules.

6. *Key Changes Introduced by the DPDP Rules when compared to the SPDI Rules*

(a) Scope:

(i) Existing Practice (*under SPDI Rules*): There is a distinction between '*personal information/data*' and '*sensitive personal information/data*', where many obligations under the SPDI Rules only apply where any sensitive personal information/data (*such as passwords, financial information, medical records, biometric information etc.*) is collected and processed.

(ii) New Requirement (*under DPDP Rules*): All personal data (*whether sensitive or otherwise*) is covered by the DPDP Rules, and all obligations will apply to the Data Fiduciary regardless of the kind of personal data collected from Data Principals. The scope of the DPDP Rules is wider when compared to the SPDI Rules in relation to personal data or sensitive personal data, since there is no longer a classification of '*sensitive personal data*' and '*personal data*'.

(b) Consent and Notice:

(i) Existing Practice (*under SPDI Rules*): Data Fiduciaries need to obtain written consent (*via letter, fax, or email*) from the Data Principal prior to collecting any sensitive personal data from such Data Principal, and also maintain a privacy policy for handling of or dealing in personal information provided by Data Principals. There is no concept of an independent '**notice**' which must precede or accompany consent.

(ii) New Requirement (*under DPDP Rules*): Data Fiduciaries will need to obtain free, specific, informed, unconditional and unambiguous '**consent**' with a clear affirmative action (*i.e., the Data Principal must actively provide assent, for example, by ticking a box, clicking a consent button, or signing digitally, rather than consent being deemed to be provided because they passively continued to use any service, or were automatically opted in*) from the Data Principal prior to collecting any personal data from them. Additionally, such consent must be accompanied or preceded by a '**notice**' to the Data Principal informing them about the personal data being collected, purpose for collection, manner of exercising data principal rights, and manner of making a complaint to the DPB. The contents of such notice, and any request for consent, must be made available to the Data Principal (*at their option*), in English or any of the 22 (twenty-two) official languages of India. Notice and consent are independent and standalone action items required for processing.

(c) Breach Notification:

(i) Existing Practice (*under SPDI Rules*): There is no express mechanism or timeline specified for the notification of any personal data breach under the SPDI Rules, however, the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties), 2013. ("CERT-In Rules"), read with the CERT-In Directions dated April 28, 2022, related to '*information security practices, procedures, prevention, response, and reporting of cyber incidents for Safe & Trusted Internet*' ("CERT-In Directions"), provides for the mandatory reporting of certain '*cyber incidents*' (*as provided for in Annexure I of the CERT-In Directions*) by Data Fiduciaries to the Indian Computer Emergency Response Team ("CERT-In") within 6 (six) hours of becoming aware of such incidents. This includes data breach, data leak, spoofing, phishing attacks, etc., and is wide enough to also encompass personal data breaches as well.

(ii) New Requirement (*under DPDP Rules*): In addition to the CERT-In reporting mechanism provided under the CERT-In Rules and CERT-In Directions, a personal data breach triggers a 3 (three) layer reporting obligation on the Data Fiduciary under the DPDP Rules: **(A)** first, the affected Data Principals must be notified about certain particulars regarding the breach without delay through their registered communication channels; **(A)** second, the DPB must be provided an initial notification without delay, as soon as the Data Fiduciary becomes aware of the breach; and **(C)** lastly, a subsequent detailed notification must then be submitted to the DPB within 72 (seventy-two) hours (*or later if formally extended*) of becoming aware of the breach, outlining the circumstances of the breach, mitigation measures, remedial action, confirmation of notifications issued to impacted Data Principals etc.

(d) Data Principal Rights:

(i) Existing Practice (*under SPDI Rules*): Data Principals only have the right to: **(A)** review and correct personal data provided, and **(B)** withdraw consent for processing data provided.

(ii) New Requirement (*under DPDP Rules*): Data Principals will have more comprehensive rights in relation to their personal data, as follows: **(A)** right to access information about personal data already provided; **(B)** right to correct, complete, update, and seek erasure of personal data already provided; **(C)** right to redress grievances with the Data Fiduciary first, then approach the DPB for further redressal if the Data Fiduciary fails to do so at the first instance, and **(D)** right to nominate an individual who will be able to exercise such Data Principal's rights, in the event of death or incapacity of the concerned Data Principal.

(e) Basis for Processing Personal Data:

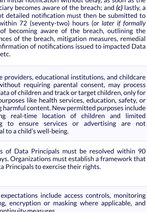
(i) Existing Practice (*under SPDI Rules*): Data Fiduciaries may simply process personal data on the basis of '*written consent*' obtained from the Data Principal.

(ii) New Requirement (*under DPDP Rules*): Data Fiduciaries will be permitted to process personal data: **(A)** with consent obtained by affirmative action from the Data Principal, or **(B)** without consent (i.e., '*legitimate use*'), such as for employment-related purposes, for a specified purpose if the data principal has voluntarily provided such data, for responding to medical exigencies or public health threats, for performing any function/obligation under law, for the State providing any service or benefit to the Data Principal, for compliance with any judgment or order issued under any law, etc. In either case, such processing must be for a '*lawful purpose*'.

(f) Children's Personal Data:

(i) Existing Practice (*under SPDI Rules*): The SPDI Rules do not provide for any additional requirements in relation to the processing of personal data of children.

(ii) New Requirement (*under DPDP Rules*): Data Fiduciaries will be required to obtain '*verifiable consent*' from the parent (*or guardian, wherever applicable*) of a child (*by adopting appropriate technical and organisational measures and exercising due diligence for this purpose*) or a person with disability (*by exercising due diligence to verify court documents appointing their lawful guardian*), before processing such child's/disabled person's personal data, subject to certain exemptions provided in the DPDP Rules.



7. *Important Obligations on Data Fiduciaries which will come into effect from May 13, 2027*

Compliance Area	Key Requirement under the DPDP Act	What the DPDP Rules Add	Practical Action Items for Organisations
Notice	A notice must be provided before or at the time of seeking consent, describing the personal data collected, purpose, grievance process, and Data Principal rights, and must be made available to Data Principals (*at their option*) in English or any of the 22 (twenty-two) official languages of India.	Notices must itemise personal data categories to be processed; specify purpose of such processing and provide a specified description of goods/services enabled; and include links for withdrawal, exercising Data Principal rights and making complaints to the DPB.	Re-design notices so they are standalone, purpose-specific, and multi-lingual. Ensure notices contain withdrawal mechanisms and rights-access links.
Consent	Personal data may be processed only on the basis of valid consent or a recognised legitimate-use ground. Consent must be free, specific, informed, unconditional, unambiguous, and provided through clear affirmative action. Existing consents (*i.e., those given by Data Principals prior to May 13, 2027*) remain valid until withdrawn, provided the Data Fiduciary as soon as reasonably practicable, provide such Data Principals with a notice.	Fresh notice and consent required when introducing new purposes or collecting new data points. Withdrawal must be as easy as giving consent.	Identify legacy datasets processed on the basis of previously obtained consent. Issue fresh notices where processing continues for existing, new or additional purposes. Align all new consent flows to the DPDP standard.
Legitimate Uses (*Non-Consent Based Processing*)	Without consent, personal data may be processed for limited situations such as public/health emergencies, medical treatment, employment administration, compliance with law, and court orders etc.	No expansion of categories; organisations are expected to assess, record, and justify the use case.	Conduct a mapping exercise to identify processing dependent on legitimate use.
Retention and Deletion	Personal data must be retained only as long as necessary for the purpose collected or as required under law. Data must be deleted when consent is withdrawn or the purpose is served.	Minimum retention of personal data, traffic data and processing logs for 1 (one) year after purpose completion or withdrawal.	Establish purpose-based retention schedules. Deploy deletion workflows triggered by withdrawal or purpose expiry. Maintain logs for a minimum of 1 (one) year.
Data Breach Notification	Data Fiduciaries must notify affected individuals and the DPB of any personal data breach.	A personal data breach triggers a 3 (three) layer reporting obligation on the Data Fiduciary: **(a)** first, the affected Data Principals must be notified about certain particulars regarding the breach without delay through their registered communication channels; **(b)** second, the DPB must be provided an initial notification without delay, as soon as the Data Fiduciary becomes aware of the breach; and **(C)** lastly, a subsequent detailed notification must then be submitted to the DPB within 72 (seventy-two) hours (*or later if formally extended*) of becoming aware of the breach, outlining the circumstances of the breach, mitigation measures, remedial action, confirmation of notifications issued to impacted Data Principals etc.	Establish breach reporting SOPs; designate internal reporting channels; require Data Processors to notify breaches immediately; align with CERT-In and sectoral obligations.
Processing of Personal Data of Children/ Persons with Disabilities	Verifiable parental or lawful guardian consent required. Processing cannot harm well-being.	Healthcare providers, educational institutions, and childcare settings, without requiring parental consent, may process personal data of children and track or target children, only for specified purposes like health services, education, safety, or preventing harmful content. New permitted purposes include determining real-time location of children and limited monitoring to ensure services or advertising are not detrimental to a child's well-being.	Implement age/identity verification. Implement parental consent mechanisms. Disable tracking and targeted advertising where applicable.
Data Principal Rights	Data Principal rights include access, correction, completion, update, erasure, nomination, and grievance redressal.	Grievances of Data Principals must be resolved within 90 (ninety) days. Organizations must establish a framework that allows Data Principals to exercise their rights.	Establish Data Principal rights-handling workflows, identity verification, tracking, and response systems. Publish processes and contact information.
Reasonable Security Practices	The DPDP Act requires reasonable security measures to prevent personal data breaches.	Minimum expectations include access controls, monitoring and logging, encryption or masking where applicable, and business continuity measures.	Implement access controls, logging, encryption, incident response, and backup regimes. Test business continuity and recovery mechanisms.
Cross-Border Data Transfers	Transfers of personal data to jurisdictions outside India are permitted unless restricted by notification of the Central Government, pertaining to blacklisted territories.	Transfers of personal data to jurisdictions outside India are permitted provided that Data Fiduciaries comply with any conditions/restrictions notified by the Central Government.	Review agreements and ensure contracts allow modification if transfer conditions change.
Control over Data Processors	Data Fiduciaries remain responsible for Data Processors' compliance.	Contracts must flow obligations down to processors, including security, breach support, deletion and cooperation.	Amend vendor/service provider contracts to ensure flow down DPDP Act compliant obligations, including security, breach support, deletion/return, log retention and cooperation duties. Require audit and cooperation rights. Prohibit onward transfers without approval.
Significant Data Fiduciaries	Certain Data Fiduciaries may be designated by the Central Government as SDFs based on volume/sensitivity of personal data being processed, security of the State etc.	SDFs must appoint a data protection officer (DPO) (*India-based*), conduct annual audits and data protection impact assessments (DPIAs), implement algorithmic due diligence, and comply with data localisation if mandated.	Monitor for designation of SDFs by the Central Government. If designated, restructure governance, undertake audits and DPIAs, appoint a DPO based in India, and adhere to any data localisation requirements.
Retention by E-Commerce Entities, Social Media Intermediaries and Online Gaming Intermediaries	Not addressed under the DPDP Act.	E-commerce entities, social media/online gaming intermediaries with large Indian user bases beyond thresholds mentioned in the DPDP Rules, must delete personal data after 3 (three) years of user inactivity and provide 48 (forty-eight) hour prior notice.	Verify whether user thresholds under the DPDP Rules are met. Implement automated inactivity tracking and pre-deletion notice protocols.

8. *Provisions for Consent Managers which will come into effect from November 13, 2026*

The DPDP Act creates a new regulated category: '*consent managers*'. These entities are registered with the DPB and act as a single interface through which Data Principals can give, manage, review, or withdraw consent. The platform operated by consent managers must be accessible, transparent, interoperable, and data blind, meaning they cannot view the contents of any personal data routed through them. To qualify as a consent manager, an organisation must meet eligibility criteria set out in the DPDP Rules, including being incorporated in India, having a minimum net worth of INR 20,000,000 (twenty million), and demonstrating adequate technical and financial capability, along with management that meets prescribed reputation and integrity standards.

The DPDP Rules impose additional structural, governance, and regulatory obligations on consent managers, requiring that their statutory duties be expressly incorporated into their constitutional documents, with any amendments or transfer of control (*including mergers or sales*) subject to prior approval of the DPB. Consent managers are also subject to DPB oversight, including audit and suspension powers, and must publicly disclose detailed ownership and management information, including holdings above prescribed thresholds. Consent managers must support interoperable consent flows between multiple onboarded Data Fiduciaries, act in a fiduciary capacity toward Data Principals, retain records for a minimum of 7 (seven) years, and are prohibited from subcontracting or assigning their obligations.

Consent managers are further required to: **(a)** implement safeguards to avoid conflicts of interest with Data Fiduciaries, including conflicts linked to directors or senior leadership; **(b)** maintain detailed records of consent-related activities for no less than seven years; and **(c)** adopt security and technical measures ensuring personal data transmitted via their platform remains unreadable to the consent manager.

These registration requirements and operational obligations surrounding consent managers will become effective from November 13, 2026.

9. *Action Items for Compliance which will come into effect from May 13, 2027*

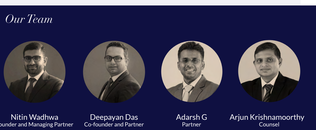
Data Fiduciaries must ensure the following action items are in place from May 13, 2027, to comply with the DPDP Act and DPDP Rules

(a) Prepare a detailed inventory of all personal data that is processed to determine whether the DPDP Act applies;
(b) Review all activities related to data processing to verify whether any of such activities can be classified as a legitimate use;
(c) Prepare notice templates that contains all such details as are necessary for the Data Principal to make an informed consent;
(d) Implement a mechanism to obtain verifiable parental consent for processing data of children and persons with disabilities;
(e) Cease tracking, behavioural monitoring, or targeted advertising towards children if engaged in business that collects personal data of children;
(f) Prepare and enforce purpose-based data retention policies;
(g) Put in place reasonable security practices and measures for protection of personal data;
(h) Prepare documentation setting out internal procedures to enable Data Principals to exercise their rights;
(i) Prepare a data breach response plan that includes reporting protocols to the DPB and to the affected Data Principal;
(j) Review all data transfer arrangements to align with government specified conditions, as and when they are issued;
(k) If likely to be classified as an SDF, appoint a DPO in India, establish procedures for impact assessments and audits and account for data localisation requirements; and
(l) If planning to operate as a consent manager, ensure that you meet the eligibility criteria, and put in place requirements to manage consent in a transparent manner, prior to November 13, 2026.

10. *Way Forward*

The notification of the DPDP Rules marks the final step in operationalising India's first dedicated data protection regime, translating broad statutory principles into concrete operational requirements. The flexibility to design consent protocols and build privacy-by-design frameworks sits alongside obligations that carry limited interpretive space, particularly the 1 (one) year minimum retention requirement, restrictions linked to children's personal data, and the possibility of additional controls around data localisation and cross-border transfers. The 18 (eighteen) month implementation window therefore represents both opportunity and obligations on organisations to move decisively from identifying issues to executing operational changes, such as mapping data flows, amending notices and contracts, restructuring consent and rights mechanisms, recalibrating security and breach response processes, and assessing exposure to SDF designation. This is not solely a compliance exercise, but rather a structural re-architecture of data governance, offering a chance to embed trust, resilience, and accountability into digital products before enforcement becomes active and scrutiny increases.

Our Team



Nitin Wadhwa
Founder and Managing Partner

Deepayan Das
Co-founder and Partner

Adarsh G
Partner

Arjun Krishnamoorthy
Counsel

For any questions or assistance that you may require on the matter, please feel free to contact the Firm's Founder and Managing Partner at nitinwadhwa@wadhwa.in or call him directly at +91 98992 19933.