MONTHLY BULLENTIN

DECEMBER, 2025

CLASIS LAW

DATA PRIVACY SPECIAL

TOLSTOY HOUSE, 4TH FLOOR, TOLSTOY MARG,
NEW DELHI – 110001, INDIA TEL : +91 11 4213 0000

SEASON'S GREETINGS

As Christmas approaches and we prepare to welcome the New Year, we extend our warmest greetings and best wishes to all our valued clients. This festive season is a time of reflection, gratitude, and renewed optimism, providing an opportunity to look back on the year past and ahead to the possibilities of the year to come.

Christmas is a season that reminds us of the importance of goodwill, compassion, and strong relationships. These values are the fundamental to the way we work and to the long-term partnerships we strive to build with our clients. As we look ahead to the New Year, we remain committed to being your trusted legal partners. We hope this festive season brings you joy, new opportunities and celebration with family and loved ones.

We wish you a Merry Christmas and a very Happy New Year.

2026

BEHIND THE BUZZWORDS: REAL-WORLD IMPLICATIONS OF INDIA'S DPDP LAW

India's digital landscape has undergone rapid transformation, bringing both opportunities and challenges in safeguarding personal data. In response, the Government of India enacted the Digital Personal Data Protection Act, 2023 (the "**Act**"), a landmark legislation aimed at protecting individuals' digital privacy on August 11, 2023. After a long wait, the Digital Personal Data Protection Rules (the "**Rules**") were notified on November 13, 2025, a necessary step to provide the operational clarity and guidance for the stakeholders to implement the provisions of the Act.

The Rules serve as the operational backbone of the Act, translating its principles into specific compliance obligations. They outline key requirements for data fiduciaries such as consent management, data security, breach reporting and cross-border data transfers while also defining the rights of data principals and the role of the Data Protection Board (the "**Board**"). In this article, we will examine several of these core provisions and their implications for stakeholders in India's digital ecosystem.

Applicability and Commencement Timeline

Acknowledging the significant obligations and the time that would be required by stakeholders for implementation under the Act and Rules, (the "**DPDP regime**"), the Government has adopted a phased approach to operationalize the provisions. This structured implementation framework divides the commencement into 3 distinct stages to allow a smooth transition across the ecosystem.

a. Effective Immediately: The first phase operationalizes Rules 1, 2, and 17 to 21, which lay the institutional foundation for the DPDP regime. These provisions include the applicability, key definitions and detailed provisions relating to the constitution and functioning of the Board[1]. This phase ensures that the primary regulatory authority – the Board, envisaged under the DPDP regime is constituted and made operational without delay.

b. Effective 1 Year from Notification: The second phase will bring Rule 4 into force after 1 year from the date of notification, prescribing the framework for registration and operational obligations of consent managers[2]. This mandates their formal recognition and adherence to defined technical and governance standards for managing and facilitating consent on behalf of data principals under the DPDP regime.

c. Effective 18 Months from Notification: The final phase, commencing 18 months after publication, will operationalize the remaining provisions[3].These Rules complete the compliance framework under the DPDP regime, covering notice obligations, lawful processing for public services, mandatory personal data breach notifications, security safeguards, enforcement of data principal rights, grievance redress mechanisms and other key operational requirements. This phase signifies the full implementation of the complete DPDP regime, bringing the entire regulatory framework into effect.

Immediate enforcement of governance Rules ensures quick oversight. Consent managers have 1 year to establish frameworks, while business especially major fiduciaries have 18 months to prepare and comply with the core obligations.

Processing of Personal Data

A person may process the personal data of a data principal only in accordance with the DPDP regime and only for a lawful purpose[4], either pursuant to the data principal's consent or for specified legitimate uses.

i. **Requirement of consent** - Where processing is based on consent, such consent must be free, specific, informed, unconditional, unambiguous and given through a clear affirmative action, accompanied by a notice that explains the purpose of processing, the rights available to the data principal and the manner of raising complaints. The data principal must also have the ability to withdraw consent at any time with comparable ease[5].

ii. **Legitimate use** - Separately, the Act recognises specified legitimate uses where personal data may be processed without consent, including processing for a purpose voluntarily initiated by the data principal, delivery of state-provided services or benefits, performance of statutory functions, compliance with legal obligations or court orders, medical emergencies, public health situations, disaster response and certain employment-related purposes[6].

Consent Managers

The Act defines a "Consent Manager" as a person registered with the Board who serves as the point of contact for a data principal. It further specifies the role of the consent manager as follows:

i. serving as the single point of contact for the data principal to facilitate the giving, management, review and withdrawal of consent.
ii. providing an accessible, transparent and interoperable platform for consent management[7].
iii. accountability to the data principal[8] and acting on her behalf in accordance with the obligations prescribed by the Board[9].
iv. ensuring protection, security and integrity of the data principal's consent throughout its lifecycle.

Every consent manager meeting the eligibility criteria[10] is to be registered with the Board in accordance with the procedures, laid down by the Board and such registration shall be subject to meeting the technical, operational, financial and other conditions prescribed from time to time. The Board would monitor compliance by consent managers.

Schedule I (B) of the Rules provide for detailed obligations of the consent manager which include enabling and managing consent for data principals, ensuring data confidentiality and security, maintaining and providing access to consent and data-sharing records and retaining records for 7 years, avoiding conflicts of interest, acting in a fiduciary capacity, ensuring transparency and auditability and obtaining prior Board approval for any transfer of control[11].

Data Fiduciary Obligations

The DPDP regime imposes specific obligations on data fiduciaries to ensure they process personal data in a lawful, transparent and secure manner. These obligations are critical to uphold the privacy rights of individuals and build trust in the digital ecosystem. The key obligations include:

i. **Consent Notice :** The notice provided by the data fiduciary must be standalone and easily understandable without referring to any other information. It must clearly and plainly set out all details necessary for the data principal to give specific and informed consent, including an itemised description of the personal data being collected, the specified purposes of processing, and a specific description of the goods, services or uses enabled by such processing.

ii. **Language and Accessibility :** The notice must be in clear and plain language and must provide a direct communication link to the data fiduciary's website or app, along with any other available methods through which the data principal may withdraw consent using a process as simple as giving consent, exercise their rights under the Act, or file a complaint with the Board[12].

iii. **Reasonable Security Safeguards:** Data Fiduciaries must implement reasonable security measures to protect personal data, including encryption or masking, access controls and maintaining logs to detect and respond to unauthorized access. They should ensure data backups to maintain processing in case of loss and retain logs for at least 1 year unless otherwise required by law. Contracts with data processors must include security provisions, supported by appropriate technical and organizational measures to enforce these safeguards effectively[13].

iv. **Intimation of Personal Data Breaches**

a. **Intimation to Data Principals:** Upon becoming aware of a personal data breach, the data fiduciary must without delay notify each affected data principal through their registered communication channels. The communication should be clear, concise and plain manner, detailing the nature, extent and timing of the breach. It must also explain the consequences relevant to her, that are likely to arise from the breach, the mitigation steps implemented or being implemented by the data fiduciary, recommended actions the data principal can take to protect themselves and provide contact information for a responsible representative who can address any queries[14].

b. **Intimation to the Board:** The data fiduciary is also required to inform the Board in 2 phases. First on becoming aware of a personal data breach, the data fiduciary must intimate the Board without delay, providing a description of the breach, including its nature, extent, timing, location, and likely impact. Then the second intimation within 72 hours, the data fiduciary must submit updated and detailed information in respected of such description, including the broad facts relating to the events, circumstances and reasons leading to the breach, mitigation measures implemented or proposed, any findings regarding the person responsible, remedial steps to prevent recurrence and a report on intimations issued to affected data principals[15].

v. **Specified Purpose Retention Period:** The retention obligations set clear timelines for data fiduciaries to handle personal data responsibly, striking a balance between operational requirements and privacy concerns. These Rules distinguish between large platforms with substantial user bases and other data fiduciaries, ensuring that personal data is retained appropriately and erased in a timely manner.

a. **Specific rules for certain large platforms:** Data fiduciaries including e-commerce entities, online gaming intermediaries, and social media intermediaries exceeding specified user thresholds, are required to erase personal data after 3 years of user inactivity. They must issue a 48-hour prior notice before deletion, except where retention is mandated by law or other provisions of the Act.

b. **Minimum retention for all data fiduciaries:** Regardless of size, all data fiduciaries must retain personal data, related traffic data, and relevant logs for a minimum of 1 year. This retention supports purposes such as responding to lawful requests and facilitating

investigations. After 1 year, data must be deleted unless extended retention is required by law.

Data fiduciaries outside the specified categories must evaluate when the retention purpose ends and implement appropriate policies to ensure compliance with these timelines, while respecting the minimum 1-year retention requirement[16].

vi. Contact Information for Data Processing Queries: Every data fiduciary must prominently publish on its website or app the contact details of the data protection officer or a designated representative responsible for addressing queries about personal data processing. This contact information must also be included in all communications responding to data principals exercising their rights under the Act, ensuring clear and accessible channels for inquiries related to data processing[17].

vii. Parental Consent and Guardianship for Vulnerable Individuals: Data fiduciaries must obtain parental consent before processing children's personal data and verify the adult status of the parent or guardian using reliable information, parent-provided details, or government-issued credentials[18]. Exemptions apply narrowly to specific entities like healthcare, education, and childcare and only for defined purposes such as health services, real-time location tracking, and harm prevention from targeted ads[19].

For persons with disabilities, data fiduciaries must verify lawful guardianship through court orders, designated authorities, or local committees, in line with relevant disability laws. Organisations are required to train staff to recognize these guardianship documents, reflecting the DPDP regime's focus on protecting vulnerable individuals[20].

viii. Cross-Border Data Transfers: Data fiduciaries may transfer personal data outside India but must comply with conditions imposed by the Central Government, especially concerning access by foreign states or their agencies[21]. For Significant Data Fiduciaries[22] (the "**SDFs**"), the Government based on recommendations from a designated committee[23] can specify categories of personal and related traffic data that are prohibited from being transferred abroad. While the Act generally allows such transfers, these Rules enable potential future restrictions to address national security and privacy concerns[24]. While no official notification has yet been issued specifying restricted territories for cross-border personal data transfers under the DPDP regime. The Rules state that restrictions will be based on recommendations from a committee including officials from the Ministry of Electronics and Technology and other relevant Central Government departments.

This framework attempts to strike a pragmatic balance between enabling international business operations, which are critical for multinational entities, and preserving the sovereign right of the Government to protect national security interests. However, the lack of clarity on specific territories and the criteria for restriction creates a level of uncertainty for data fiduciaries, particularly those operating across multiple jurisdictions.

Additional obligations of SDFs

In addition to obligations related to cross-border data transfers, SDFs are subject to certain additional obligations, which are as follows:

i. appoint a data protection officer who shall be based in India, will be responsible to the Board of Directors or similar governing body of the SDFs and be the point of contact for the grievance redressal mechanism[25];

ii. appoint an independent data auditor to carry out data audit, who shall evaluate the compliance of the SDFs[26].

iii. SDFs shall, once every 12 months from the date of its notification or inclusion as such,

undertake a data protection impact assessment and an audit to ensure effective compliance with the DPDP regime.

iv. SDFs shall exercise due diligence to verify that all technical measures, including algorithmic software employed for hosting, displaying, uploading, modifying, publishing, transmitting, storing, updating or sharing personal data, do not pose likely risks to the rights of data principals[27].

Administrative and Appellate Architecture of the DPDP Regime

The DPDP regime provides a structured mechanism for addressing grievances arising from the processing of personal data. Under the DPDP regime, a data principal is entitled to readily accessible grievance redressal mechanisms offered by a data fiduciary or consent manager in respect of any act or omission relating to the performance of their obligations concerning the personal data of the data principal or the exercise of the rights[28] and that such grievances must be resolved within a reasonable period, not exceeding 90 days[29].

Board - The Act establishes the Board as the government-appointed authority for enforcement of data protection laws[30], functioning primarily as a digital body[31]. The Board may take up matters through complaints, breach intimations, government references, or court directions, assess whether sufficient grounds exist, order remedial measures[32], conduct inquiries in accordance with natural justice using civil court–like powers, issue directions or penalties, close proceedings including frivolous complaints and where appropriate, refer disputes for resolution through mediation by a mutually agreed mediator[33].

Appeals - The Appellate Tribunal (the "**Tribunal**"), established under the DPDP regime, serves as the judicial authority to hear appeals against decisions of the Board. Operating as a digital office[34], the Tribunal conducts virtual hearings while upholding principles of natural justice[35] and fairness. Appeals must be filed electronically along with prescribed fees, enabling efficient and timely adjudication[36]. The Tribunal possesses powers to summon individuals, examine witnesses under oath and regulate its own proceedings.

This framework ensures data principals and entities have access to progressive administrative and appellate architecture, thereby reinforcing accountability and strengthening trust within India's evolving data protection landscape.

Penalties

The Board has the authority to impose monetary penalties after conducting a thorough inquiry and providing the affected party an opportunity to respond. In determining the penalty amount, the Board shall take into account the seriousness of the breach, type and nature of the personal data affected by the breach, duration, impact, repetitive nature, whether the person gained or avoided a loss due to the breach and efforts made to mitigate the harm[37].

Penalties under the DPDP regime vary significantly based on the nature and severity of the breach. The highest penalties, which can go up to INR 250 crore (approx. USD 30 million), apply to critical violations such as failure to implement reasonable security safeguards to prevent personal data breaches. Similarly, breaches involving failure to notify the Board or affected data principals about a personal data breach, or violations related to additional obligations concerning children, can attract penalties of up to INR 200 crore (approx. USD 24 million). SFDs may face penalties of up to INR 150 crore (approx. USD 18 million) for non-compliance with their additional obligations.

For less severe breaches, such as general obligations under the Act, penalties can be as INR 10,000 (approx. USD 120). Other violations not falling under the major categories may attract penalties up to INR 50 crore (approx. USD 6 million). Additionally, breaches of any voluntary undertakings accepted by the Board are penalized in alignment with the original breach's severity[38].

The Road Ahead: Ensuring DPDP Regime Compliance

The Rules, transform the Act's broad principles into a detailed and enforceable compliance framework, signalling a major shift toward rights-centric digital governance in India. While the Rules provide clearer operational requirements, they also bring complexity that requires businesses to act swiftly and decisively. Beyond initial issue-spotting, business must conduct thorough assessments of their data flows and move toward full-scale implementation updating policies, strengthening security measures and preparing for breach reporting and data retention obligations.

This 3-phase compliance period should be viewed as a critical runway, not a grace period. Early and proactive investment in compliance will help organizations reduce risks, meet evolving regulatory demands and build trust with increasingly privacy-aware consumers. Continuous monitoring of government notifications and the guidance from the Board will be key to navigating this evolving landscape. Ultimately, business who prioritize compliance and data governance will be best positioned to succeed in India's emerging era of robust data protection and digital accountability.

****

FOOTNOTES :

[1] Rule 1(2)
[2] Rule 1(3)
[3] Rule 1(4)
[4] Any purpose that is not expressly forbidden by law.
[5] Section 6
[6] Section 7
[7] Section 2(g)
[8] Section 6(8)
[9] Section 6(9)
[10] The applicant must be an Indian company with sound management, INR 2 crore (approx.. USD 220,000) net worth, adequate capacity, compliant governance, certified interoperable platform and operations serving Data Principals' interests.
[11] Rule Schedule I (B)
[12] Rule 3
[13] Rule 6
[14] Rule 7 (i)
[15] Rule 7 (ii)
[16] Rule 8
[17] Rule 9
[18] Rule 10
[19] Rule 12
[20] Rule 11
[21] Rule 15
[22] Section 2 (z) and Section 10 - Significant Data Fiduciary means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government on the basis of an assessment of relevant factors such as volume and sensitivity of personal data processed; (b) risk to the rights of Data Principal; (c) potential impact on the sovereignty and integrity of India; (d) risk to electoral democracy; (e) security of the State; and (f) public order.
[23] The committee responsible for these recommendations includes officials from the IT Ministry and other relevant departments.
[24] Rule 13
[25] Section 10(2)(a)
[26] Section 10(2)(b)
[27] Rule 13
[28] Section 13
[29] Rule 14
[30] Section 18
[31] Rule 20
[32] Section 27
[33] Section 31
[34] Rule 22 (3) (b)
[35] Rule 22 (3) (a)
[36] Rule 22 (2)
[37] Section 33
[38] Section 33 and Schedule

Authors: Vineet Aneja - Managing Partner, Raveena Anand - Associate Partner & Mayank Parashar - Associate.

For more information, please write to: Mr. Vineet Aneja at vineet.aneja@clasislaw.com or Ms. Raveena Anand at raveena.anand@clasislaw.com.

Notable Recognitions & Accolades

NOTABLE FIRM
BENCHMARK LITIGATION

LEADING FIRM
Legal500
ASIA PACIFIC
2025

ALB
INDIA
LAW AWARDS
2023
FINALIST
THOMSON REUTERS

AWARDS & HONORS

asialaw
2025
RANKING
LABOUR & EMPLOYMENT
NOTABLE
DISPUTE RESOLUTION
RECOGNISED

INDIA BUSINESS LAW JOURNAL
AWARD WINNING LAW FIRM
2024
LAW ASIA

LEXOLOGY
Legal Influencer
Q2 | 2022