November 2025

Digital Personal Data Protection Rules, 2025: Operationalising consent, security, and governance obligations

The Government of India has officially notified the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**") on November 13, 2025, officially published in the Gazette on November 14, 2025. The DPDP Rules enable the operationalisation of the Digital Personal Data Protection Act, 2023 ("**DPDP Act**").

The DPDP Act is India's first comprehensive, principles-based statute governing the processing of digital personal data. It applies to processing within India and extraterritorially to entities offering goods or services to individuals in India. The DPDP Act operates primarily on a foundation of explicit consent.

The DPDP Rules *inter alia* include key operational rules for Data Fiduciaries[1] ("**Data Fiduciary**") and addresses mechanisms created to protect the rights of Data Principals[2] ("**Data Principal**").

Phased commencement of key provisions

The DPDP Rules implement a staggered approach to commencement, a critical factor for global compliance planning:

Timeline	Commencement date	Implication
Immediate	November 13, 2025	Establishment of the Data Protection Board of India ("**Board**") and its operational procedures.
12 Months	November 13, 2026	The framework for the registration and detailed obligations of Consent Managers, the term used for a person registered with the Board, to act as a point of contact to enable a Data Principal to give, manage, review and withdraw consent, ("**Consent Manager**") comes into force.
18 Months	May 13, 2027	Core compliance duties apply, including notice, security safeguards, breach intimation, Significant Data Fiduciary ("**SDF**") obligations, and Data Principal rights.

[1] Data Fiduciaries is the term used for entities that determine the purpose and means of processing (analogous to 'data controllers' in other regimes).

[2] Data Principals is the term used for individuals to whom the personal data relates (analogous to 'data subjects' in other regimes).

Critical compliance obligations for Data Fiduciaries

The DPDP Rules set out the operational requirements that Data Fiduciaries must follow to implement the core obligations under the DPDP Act.

Notice and consent

The formal notice provided by a Data Fiduciary to a Data Principal must be clear, independent, and contain a 'fair account' of the processing activities. The overall framework is grounded in a notice-and-consent model, requiring DFs to disclose key processing details upfront and obtain valid consent before processing begins. The notice requires, at minimum:

1. an itemised description of the personal data to be processed;
2. the specified purpose of processing, including a specified description of the goods, services, or uses enabled; and
3. a specific communication link for Data Principals to withdraw consent, exercise other rights or make a complaint to the Board, ensuring the ease of withdrawal is comparable to the ease with which consent was given.

Business impact

Organisations will need to redesign consent flows and user interfaces to ensure consent is purpose-specific, informed with clear withdrawal pathways, or at the very least update their privacy policies to include the foregoing.

Security safeguards and breach intimation

The DPDP Rules mandate enhanced security and stringent breach reporting protocols:

1. **Mandatory security measures**: Data Fiduciaries must implement minimum safeguards, including encryption, obfuscation, masking, or the use of virtual tokens. This applies to all personal data held or controlled, including personal data processed by a Data Processor (entity processing personal data on behalf of the Data Fiduciary) ("**Data Processor**").
2. **Contractual mandate**: Contracts with Data Processors must contain appropriate provisions for implementing these reasonable security safeguards.
3. **Time-bound breach reporting**: Upon becoming aware of a personal data breach, a Data Fiduciary must:
    a) intimate and provide the Board a description of the personal data breach without delay, followed by a detailed report within 72 (seventy-two) hours; and
    b) intimate each affected Data Principal without delay, providing a description of the breach, its consequences, and mitigation measures.

Business impact

Companies will need to implement appropriate data security safeguards across all systems handling Indian personal data. Coupled with steep penalties of up to INR 200,00,00,000 (Indian Rupees two hundred crore) (~ USD 22,200,000 (US Dollars twenty-two million two hundred thousand) for reporting failures and the stringent 'without delay' notification requirement, organisations will likely need to operationalise a round-the-clock, India-aligned incident response function and incorporate strong, protective indemnity clauses in their Data Processor contracts to mitigate liability exposure.

Data retention and erasure

The purpose of limitation principle, that personal data should only be kept as long as necessary for the specified purpose, is made quantifiable for certain large-scale Data Fiduciaries:

1. **Retention period for large fiduciaries**: E-commerce entities (with a minimum of 20,000,000 (twenty million) users), online gaming intermediaries (with a minimum of 5,000,000 (five million) users), and social media intermediaries (with a minimum of 20,000,000 (twenty million users) must erase personal data (with exceptions for user account access and virtual tokens) within 3 (three) years of the date, the Data Principal last approached the Data Fiduciary for the specified purpose, unless retention is mandated by law.
2. **Mandatory log retention**: Data Fiduciaries must retain associated traffic data and other processing logs for a minimum period of 1 (one) year for forensic and investigative purposes, after which they must be erased.
3. **Erasure notice**: Data Fiduciaries must notify Data Principals at least 48 (forty-eight) hours prior to the completion of the time period for erasure, allowing the Data Principal a chance to engage with the Data Fiduciary to preserve the personal data.

Business impact

The DPDP Rules adopt a highly prescriptive approach to data retention, introducing a defined 3 (three) year deletion timeline for certain large digital platforms. This could require significant operational adjustments. Large e-commerce, gaming, and social media intermediaries will need to re-engineer data lifecycle practices, implement automated and auditable deletion workflows, and build mechanisms to track a Data Principal's 'last approach' date with precision.

Key new regulatory mechanisms

The Consent Manager framework

The Consent Manager framework is operationalised as a key intermediary to empower Data Principals:

1. **Registration criteria**: The stringent conditions ensure only trustworthy entities qualify. Requirements include: (a) incorporation in India; (b) minimum net worth of INR 2,00,00,000 (Indian Rupees two crore) (~ USD 200,000 (US Dollars two hundred thousand); (c) demonstration of sufficient technical, operational, and financial capacity; and (d) certification that its platform is interoperable and adheres to data protection standards.
2. **Fiduciary capacity**: A Consent Manager must act in a fiduciary capacity toward the Data Principal.
3. **Obligations**: Consent Managers are prohibited from sub-contracting their obligations, must avoid conflicts of interest with Data Fiduciaries. Consent Managers must retain a record of consents, notices, and data sharing activities for at least 7 (seven) years. Critically, the Consent Manager cannot read the contents of the personal data being shared.

Business impact

The Consent Manager construct, unique to the DPDP Act regime, creates a new consent orchestration layer. This introduces both compliance and architectural implications. Organisations may opt to build technical integrations with registered Consent Managers, redesign data-sharing workflows to route consent tokens through the Consent Manager ecosystem and accommodate 7 (seven) year retention requirements for consent records. Data Fiduciaries will need to establish robust governance and verification processes before relying on any Consent Manager. This necessity arises from the constraints on Consent Managers, which include inability to sub-contract, fiduciary duties towards Data Principals, and the imperative to remain conflict-free. Overall, the framework adds a significant new dependency for lawful, consent-driven processing and may materially influence product design, user experience, and backend data management practices.

SDF additional obligations

The Central Government may notify Data Fiduciaries as SDFs based on criteria like the volume and sensitivity of personal data processed. Once notified, these entities face enhanced scrutiny:

1. **Mandatory annual assessment**: SDFs must conduct a Data Protection Impact Assessment ("**DPIA**") and an audit once every 12 (twelve) months.
2. **Algorithmic due diligence**: SDFs must exercise due diligence to verify that technical measures, including algorithmic software used for processing, do not pose a risk to Data Principals' rights.
3. **Data localisation restriction**: SDFs must undertake measures to ensure that certain personal data, when specified by the Central Government, is not transferred outside the territory of India. This potential restriction is based on the recommendation of a government-constituted committee.

Business impact

While the DPIA concept mirrors elements of the General Data Protection Regulation ("**GDPR**") under European laws, the SDF designation introduces a far more intensive, India-specific compliance burden. Once classified as an SDF, an organisation needs to operationalise annual DPIAs and audits, implement ongoing algorithmic risk assessments, and prepare for the possibility of strict data-localisation obligations for categories of personal data that may be notified by the government. At the moment, there is no clarity on what additional localisation obligations will be imposed. Notably, sectoral localisation obligations, such as payments data localisation, continue to apply

International transfers and vulnerable data

Cross-border data transfer

The DPDP Rules affirm the liberalised approach to personal data transfer:

1. personal data processed under the DPDP Act may be transferred outside the territory of India; and
2. this permission is subject to any restrictions that the Central Government may specify by general or special order concerning making personal data available to any foreign State or entity under its control. This maintains the 'blacklist' approach, providing operational ease until any prohibitive list is notified.

Business impact

India's continued use of a 'blacklist' model, where cross-border transfers are permitted unless a country or entity is specifically restricted, offers far greater operational flexibility than the GDPR's adequacy and standard contractual clauses-based framework. For businesses, this could mean faster and lower-cost international data flows, with fewer contractual and assessment burdens, except in situations where additional localisation obligations are applicable to the data or entity in consideration.

Processing of child data and person with disability data

1. **Verifiable consent**: Processing the personal data of a child (an individual under 18 (eighteen) years of age) or a person with a disability requires verifiable consent from the parent or lawful guardian.
2. **Verification**: Data Fiduciaries must adopt appropriate technical and organisational measures to verify that the individual claiming to be the parent is an identifiable adult. This verification is often by reference to reliable identity and age details or a virtual token issued by an authorised entity.

3. **Exemptions**: Limited exemptions from the parental consent and protective duties are provided to certain classes of Data Fiduciaries (e.g., clinical establishments, educational institutions) for purposes such as providing health services or ensuring child safety and protection.

Business impact

The DPDP Rules require platforms, handling child or disability-related personal data to implement reliable parental consent verification systems, adding technical and operational overhead. Product flows, especially for gaming, ed-tech, and social platforms, will need stronger age-gating, guardian consent paths, and restricted processing by default. Even with limited exemptions, most businesses must introduce special handling and governance controls for such personal data to remain compliant.

Conclusion

The DPDP Rules operationalise India's new data protection regime by introducing detailed, prescriptive requirements that will require significant operational, technical, and governance adjustments for organisations processing personal data in India.

While the staggered timelines offer some room for transition, businesses, especially large digital platforms and entities likely to be designated as SDFs, will need to begin alignment efforts well in advance of the 2027 compliance date. The DPDP Rules also create new ecosystem dependencies, such as the Consent Manager framework, and introduce India-specific obligations around breach reporting, retention, and algorithmic due diligence. Overall, the DPDP framework represents a material shift toward structured and enforceable data governance, demanding early planning, cross-functional coordination, and sustained compliance readiness.

Infotech Practice

Our team understands the importance of data privacy in today's digitally interconnected world. We have dedicated our practice to ensuring that your and your customers' personal and business data remains secure, compliant, and respects the sovereignty of individuals and jurisdictions globally.

We prioritise creating bespoke solutions tailored to your business needs. We recognise that every business has unique data privacy challenges, and we use our deep understanding of international and domestic regulations to provide you with the most effective and robust legal strategies. JSA provides advice on highly sophisticated data management, data security and privacy issues. Our depth of experience gives our clients the crucial advantage of consistent and comprehensive, yet practical advice. Our Technology Law Practice group has successfully worked with several multinational organisations for the structuring and roll-out of privacy and information-security programs. We have carried out audit and risk assessments, customised global privacy and information management policies, helped create international data transfer strategies, structure and negotiate complex international data transfer agreements.

This Prism has been prepared by:

Probir Roy Choudhary
Partner

Yajas Setlur
Partner

Shivani Bhatnagar
Senior Associate

Hrishikesh Reddy Kothwal
Associate

18 Practices and
41 Ranked Lawyers

7 Ranked Practices,
21 Ranked Lawyers

14 Practices and
12 Ranked Lawyers

13 Practices and
49 Ranked Lawyers

20 Practices and
24 Ranked Lawyers

8 Practices and
10 Ranked Lawyers
Highly Recommended in 5 Cities

Regional Legal Expertise Awards (APAC) of the Year
Energy Firm Competition/
Antitrust Firm

Among Best Overall
Law Firms in India and
14 Ranked Practices

---

9 winning Deals in

IBLJ Deals of the Year

---

11 A List Lawyers in

IBLJ A-List - 2025

Recognised in World's 100 best
competition practices of 2025

Ranked Among Top 5 Law Firms in
India for ESG Practice

Asia M&A Ranking
2024 – Tier 1

For more details, please contact km@jsalaw.com

jsa
advocates & solicitors

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi