Original Research Paper

Volume - 16 | Issue - 01 | January - 2026 | PRINT ISSN No. 2249 - 555X | DOI : 10.36106/ijar

Business Administration

NAVIGATING THE PATH TOWARDS DIGITAL PERSONAL DATA PROTECTION RULES 2025 IN INDIA

Dr. V Arockia Jerold

Assistant Professor, Department of Business Administration, Loyola college.

ABSTRACT The Digital Personal Data Protection Act 2023 and the DPDP Rules 2025 embarks an important journey towards building a secured digital environment for the country. The Government of India has notified the DPDP Rules 2025 on November 13, 2025. The Act and Rules establish a citizen-focused and innovation-friendly framework for the responsible use of digital personal data. DPDP Rules 2025 is an effective tool to empower citizens for data protection and security. The study analyses the obligation of Data fiduciaries, Data principals, Data security , Individual rights and penalties for non compliance. The amended rules will transform India towards a safer, more transparent and innovation-friendly data ecosystem that serves citizens and strengthens public confidence in digital governance.

KEYWORDS : Digital Personal Data Protection Act 2023, Digital Personal Data Protection Rules 2025, Digital personal and Data protection

INTRODUCTION:

The DPDP Act, 2023 establishes India's first comprehensive data protection framework, balancing privacy rights with lawful data processing. The Digital Personal Data Protection Act was enacted by Parliament on August 11, 2023, establishing principles for protecting citizens' digital information. The DPDP Act was approved by the President on August 11, 2023. On January 3, 2025, Ministry of Electronics and Information Technology released the draft DPDP Rules in the Gazette of India, inviting public consultation until February 18, 2025. These rules operationalize the Digital Personal Data Protection (DPDP) Act, 2023, India's first dedicated law for digital privacy. The Act and Rules establish a citizen-focused and innovation-friendly framework for the responsible use of digital personal data. The 2025 Draft Rules enhance compliance, introduce digital grievance redressal, and permit cross-border data flows, aligning with global standards like the EU's GDPR while addressing local needs. The Act required operational rules to become functional. The DPDP Rules 2025 provide procedures, timelines, and compliance requirements. The framework is built on seven core principles: consent and transparency, purpose limitation, data minimisation, accuracy, storage limitation, security safeguards, and accountability.

Significance Of The DPDP RULES 2025

The DPDP Rules 2025 are significant because they make India's data protection law fully operational by translating the DPDP Act into enforceable procedures. They give practical shape to citizen rights, ensure that consent is taken and managed properly, and mandate clear standards for data security, breach reporting, and data retention. By setting specific obligations for Data Fiduciaries and Significant Data Fiduciaries, the Rules create accountability across digital platforms. They also strengthen protections for children and enable smoother grievance redressal through the Data Protection Board. Overall, the Rules turn India's privacy framework from a policy commitment into a functioning system that improves trust, transparency, and responsible data use.

Evolution Of Right To Privacy In India

YEAR	CASES – RIGHT TO PRIVACY IN INDIA
1950	AK Gopalan Case - The Supreme Court rejected the argument regarding the right to privacy.
1962	Kharak Singh Case - It was the first instance where the Supreme Court of India granted relief based on the Right to Privacy, though it did not formally recognize it as a fundamental right at the time.
2011	A.P. Shah Committee - It recommended comprehensive privacy legislation, proposing a unified law to protect privacy and personal data in both private and public sectors.
2017	Justice K S Puttaswamy (Retd) vs Union of India Case - The Supreme Court unanimously affirmed that the right to privacy is a fundamental right inherent to life and liberty under Article 21.

Global Practices On Data Governance

COUNTRY	LAW ON DATA GOVERNANCE
European Union	The EU's General Data Protection Regulation (GDPR) is a comprehensive law protecting personal data, recognizing privacy as a fundamental right that safeguards individual dignity and control over personal information.
China	The Data Security Law (DSL) mandates classifying business data by importance and imposes new restrictions on cross-border data transfers. The Personal Information Protection Law (PIPL) grants Chinese data principals new rights to prevent the misuse of personal data.
United States	T The US lacks a comprehensive privacy law like the EU's GDPR, relying instead on sector-specific regulations. Government data use is governed by broad laws like the Privacy Act, while the private sector follows limited, sector-specific rules.

Key Provisions Of The Draft DPDP Rules, 2025

Notice and Consent Protocols : Consent is central to the DPDP framework. Rule 3 specifies the content and format of the notice that data fiduciaries must provide to data principals. The notice must be clear, self-contained, and list the following parameters: (i) Data categories and purpose: An itemized description of the personal data to be collected or processed, and the specific purpose(s) of such processing. (ii) Service description: A clear explanation of the goods or services enabled by the processing. (iii) Withdrawal link and rights: A direct communication link for withdrawing consent, along with information on how to exercise rights under the Act and lodge complaints.

State Processing and Security: Rule 5 requires state-driven processing of personal data to comply with standards in the Second Schedule. These standards align with basic data protection principles, including lawful use, purpose limitation, accuracy, storage limitation, and security safeguards. Rule 6 imposes a general security safeguard duty on every data fiduciary, requiring "reasonable security safeguards" to prevent breaches. This includes: Encrypting or tokenizing data, Strict access control to computers and networks, Maintaining logs and monitoring access for intrusion detection, Retaining logs and data backups for at least one year to investigate breaches, Contractual safeguards for third-party processors

Data Breach Reporting: Rule 7 establishes a data breach notification regime. Data fiduciaries must promptly inform affected data principals of any personal data breach in a clear and plain manner, describing the nature and timing of the breach, its likely consequences, and mitigation steps. The fiduciary must also notify the Data Protection Board within 72 hours of becoming aware of the breach, providing details including the breach description, its likely impact, mitigation steps, and findings on the cause or perpetrators.

Data Erasure: Rule 8 instructs certain data fiduciaries listed in the Third Schedule to erase personal data when it is no longer needed. The

Third Schedule sets fixed periods for different sectors, typically three years from the last user interaction or the Rules' commencement. Data retention is allowed for up to three years from the last interaction with the Data Principal or the effective date of the rules, whichever is later. The Data Fiduciary must notify the Data Principal at least 48 hours before erasure.

Data Principal and Grievances: Rule 9 requires every fiduciary to prominently publish the contact information of the Data Protection Officer or other person who can answer principals' questions about their data. Rule 14 focuses on how principals exercise rights, mandating fiduciaries and consent managers to publish the means by which a principal may make a rights request. All data fiduciaries and consent managers must commit to resolving principal grievances within 90 days and must publish this timeline

Significant Data Fiduciaries: Rule 13 adds extra obligations for Significant Data Fiduciaries, mandating annual Data Protection Impact Assessments (DPIAs) and compliance audits, with findings reported to the Data Protection Board. These major fiduciaries must also observe due diligence to ensure their technical measures do not endanger principals' rights.

Transfers and Exemptions: Rule 15 states that personal data may leave India's borders only if the data fiduciary meets conditions specified by the central government. Rule 16 echoes the Act's broad research and archival exemption, providing that the Act's obligations do not apply to personal data processing for research, archiving, or statistical purposes if done according to the Second Schedule standards.

Data Protection Board and Governance : Rules 17-19 lays out the Data Protection Board's constitution. A Search-cum-Selection Committee recommends a Chairperson, and a similar committee recommends the other four members. The government then appoints them. The Board's procedures follow standard collegial norms, and the Board can adopt "techno-legal measures" to conduct all its business digitally.

Consent Managers: The digital platform may also collect consent through consent managers. A Consent Manager must be an Indian company with a minimum net worth of Rs 2 crore, responsible for managing the collection, storage, and use of user consent in data privacy and digital interactions.

PHASED IMPLEMENTATION

The government has adopted a phased rollout of the Act spanning 18 months. This timeline allows businesses time for transition while establishing enforcement mechanisms. Certain provisions of the Act such as establishment of the Data Protection Board of India became effective November 14, 2025. Data fiduciaries (organizations handling personal data) have until November 2026 to comply with certain provisions, including disclosing their Data Protection Officer details. The Consent Manager framework for data removal and amendment rights will also launch then. Major tech firms will have up to 18 months until full enforcement to ensure compliance.

EMPOWERING CITIZENS THROUGH CONSENT AND TRANSPARENCY

At the heart of the privacy policy of India lies informed consent. The DPDP Rules mandate that Data Fiduciaries obtain clear consent before collecting personal data. Pre-ticked boxes, bundled permissions, or implied consent are prohibited. Organizations must issue consent notices in English or any of the 22 scheduled languages. These notices must specify what data is being collected, why it's needed, and how citizens can withdraw consent and exercise their rights. The framework establishes Consent Managers, entities registered with the Data Protection Board to help individuals manage permissions across services. Consent Managers must be Indian companies meeting technical and security standards. Additionally, the framework grants citizens four rights: access to their data, correction of inaccuracies, erasure when no longer needed, and the ability to nominate someone to exercise these rights on their behalf. Data Fiduciaries must respond to such requests within 90 days.

MANAGING CROSS-BORDER DATA TRANSFERS

Cross-border transfer of personal data under the Act is permitted but tightly regulated. A Data Fiduciary may transfer personal data outside India only if it fulfils the conditions laid down by the Central Government. These conditions may include restrictions on making such data available to any foreign State, its agencies, or entities under its control. Additionally, processing of personal data for the purposes like research, archiving and statistical studies is exempt from the Act, provided it adheres to the standards listed in the Second Schedule. This ensures that data-driven research and knowledge-building can continue without undue compliance burdens, while still maintaining essential safeguards.

DIGITAL ENFORCEMENT THROUGH THE DATA PROTECTION BOARD

The Data Protection Board of India functions as a digital institution, enabling citizens to file and track complaints online through platforms and mobile applications. The DPBI will have four members appointed by Ministry of Electronics and Technology. The board can investigate complaints and impose penalties for data breaches, though members haven't been selected yet. This approach promotes transparency, efficiency, and access. Citizens must first file grievances with the Data Fiduciary. Only if unresolved within 90 days can complaints escalate to the Board. This approach reduces regulatory burden while ensuring organizations maintain grievance redressal mechanisms. The Board has enforcement powers, including authority to impose penalties up to ₹250 crore per instance for violations. Appeals against Board decisions lie with the Appellate Tribunal, TDSAT (Telecom Disputes Settlement and Appellate Tribunal), ensuring judicial oversight.

CONCLUSION:

The Digital Personal Data Protection Act and the DPDP Rules mark an important step in building a trustworthy and future-ready digital environment for the country. They bring clarity to how personal data must be handled, strengthen the rights of individuals and create firm responsibilities for organizations. The framework is practical in design and backed by wide public consultation, which makes it both inclusive and responsive to real needs. It supports the growth of India's digital economy while ensuring that privacy remains central to its progress. The amended rules on Data protection provides a transparent and innovation-friendly data ecosystem that serves citizens and strengthens public confidence in digital governance.

REFERENCES:

1. DPDP Rules 2025
2. https://www.meity.gov.in
3. https://static.pib.gov.in