



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

DATA PROTECTION IN INDIA AFTER THE DPDP ACT, 2023: A CRITICAL ANALYSIS

Mudit Vikaram Singh

ABSTRACT

The rapid expansion of digital technologies, on line platforms, synthetic intelligence, virtual payments, e-commerce and records-pushed governance has transformed private data into a critical monetary and social useful resource. At the identical time, giant collection and processing of personal information have created vast dangers regarding privacy, surveillance, profiling, identification robbery, discrimination and unauthorized disclosure. In India, the constitutional recognition of privacy as a fundamental proper in Justice **K.S. Puttaswamy (Retd.) v. Union of India** marked a crucial development inside the prison protection of informational privateness. The subsequent enactment of the Digital Personal Data Protection Act, 2023 (“DPDP Act”) represents India's foremost legislative try to set up a complete framework governing the processing of digital private statistics.

The DPDP Act introduces standards along with the “Data Principal,” “Data Fiduciary,” “Consent Manager,” “Significant Data Fiduciary,” and the Data Protection Board of India. It establishes duties regarding notice, consent, security safeguards, breach notification, kid's information, complaint redressal and deletion of private facts. It additionally gives large monetary consequences for certain contraventions. The Digital Personal Data Protection Rules, 2025 further difficult the operational framework with the aid of prescribing necessities regarding notices, consent management, security safeguards, breach notifications, kid's statistics, Significant Data Fiduciaries and other compliance topics.

Keywords: Data Protection, Digital Personal Data, DPDP Act, Privacy, Data Fiduciary, Data Principal, Consent, Data Protection Board, Informational Privacy, Cyber Law.

INTRODUCTION

Personal records has come to be one of the maximum treasured resources inside the virtual economic system. Individuals automatically provide data to banks, hospitals, educational establishments, telecommunications organizations, e-trade structures, social-media offerings, employers, government groups and technology organizations. The increasing integration of synthetic intelligence, cloud computing, biometric identification, virtual payments and algorithmic selection-making has in addition increased the scale and complexity of private-statistics processing.

The prison importance of private statistics extends beyond commercial confidentiality. Personal records may also reveal a character's identity, area, monetary situations, fitness information, possibilities, relationships, communications and on line behavior. Unauthorized processing can also consequently affect dignity, autonomy, equality and person freedom.

The Indian constitutional function changed considerably with the Supreme Court's nine-judge selection in Justice K.S. Puttaswamy (Retd.) v. Union of India. The Court unanimously recognized privacy as a constitutionally covered right bobbing up mainly from Article 21 and the guarantees of Part III of the Constitution. The judgment specially identified informational privacy as an important size of privacy and determined the need for a felony framework able to protective personal statistics.¹

The Supreme Court's next selections have also emphasized legality, legitimate nation objectives, necessity and proportionality whilst essential rights are restricted.²

Before the DPDP Act, India did not have a complete standalone personal-information safety statute. The Information Technology Act, 2000 ("IT Act") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") furnished a sectoral confined framework. Section 43A of the IT Act imposed liability on positive frame corporates for negligent failure to maintain reasonable

¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India). The Supreme Court recognized privacy as a constitutionally protected fundamental right and discussed informational privacy as an important dimension of the right. The Supreme Court's official materials identify the judgment as the landmark nine-judge privacy decision.

² *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2018) 12 SCC 1 (India) (Aadhaar). The Court examined, inter alia, collection, storage, retention and use of residents' data and the constitutional implications of data protection and surveillance.

security practices regarding touchy non-public statistics.³ The framework become however narrower than contemporary comprehensive information safety regimes.

The DPDP Act, enacted in 2023, consequently represents an important alternate in India's legislative method. Its lengthy title states that it seeks to alter processing of virtual private statistics whilst recognizing both the right of people to defend non-public records and the want to process personal records for lawful functions.⁴

The Act was accompanied via the Digital Personal Data Protection Rules, 2025 ("DPDP Rules"), which offer distinct implementation necessities. The Rules were notified on November 13, 2025, and establish a phased commencement mechanism. Rules 1, 2 and 17–21 got here into force upon booklet, Rule four after one year, and Rules 3, 5–16, 22 and 23 after eighteen months.⁵

The put up-DPDP criminal framework should consequently be understood now not simply as the enactment of a brand new statute but as the improvement of an institutional and regulatory system governing the collection, use, storage, sharing and deletion of virtual private data.

EVOLUTION OF DATA PROTECTION LAW IN INDIA

THE PRE-DPDP FRAMEWORK

India's pre-DPDP framework changed into dispersed across numerous statutes and regulatory gadgets. The IT Act turned into often designed to provide prison recognition to electronic transactions and cope with cyber offences. It became not at first conceived as a complete privacy statute.

Section 43A of the IT Act sooner or later delivered a shape of statistics-protection legal responsibility. Where a frame corporate possessing, managing or coping with touchy private statistics or records negligently didn't hold reasonable protection practices and techniques and

³ Information Technology Act, No. 21 of 2000, § 43A, India Code (2000). Section 43A addresses compensation for failure by a body corporate to maintain reasonable security practices concerning sensitive personal data or information.

⁴Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023). The Act was enacted on August 11, 2023.

⁵ Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), r. 1 (Nov. 13, 2025). The Rules establish a phased commencement mechanism, with different provisions taking effect immediately, after one year or after eighteen months.

consequently brought about wrongful loss or wrongful gain, it is able to be at risk of pay repayment.⁶

The SPDI Rules supplemented section 43A by using defining touchy non-public facts or data and implementing necessities regarding privacy policies, consent, collection, purpose quandary, disclosure and safety practices.⁷

Although these provisions provided an important basis, that they had huge limitations. They centered appreciably on “sensitive personal records or data,” carried out principally to targeted entities and did now not set up a complete rights-primarily based data safety authority comparable to fashionable information safety regulators.

The absence of a comprehensive framework became increasingly huge as India's virtual economic system accelerated.

CONSTITUTIONAL RECOGNITION OF PRIVACY

The constitutional basis for facts safety is closely related to the Supreme Court's decision in Puttaswamy. Before that selection, Indian privacy jurisprudence had advanced incrementally via selections concerning physical autonomy, seek and seizure, communications and personal liberty.

In Justice K.S. Puttaswamy (Retd.) v. Union of India, the nine-decide Bench held that privacy is a constitutionally protected proper. The judgment recognized privacy as a crucial issue of dignity, liberty and autonomy.⁸

Importantly, privateness become no longer limited to physical or spatial privacy. Informational privacy issues and character's capacity to exercise manipulate over data concerning themselves. In an increasingly digitized society, this precept gives a constitutional basis for regulating the collection and use of private statistics.

The popularity of privateness, however, does not imply that every processing of private information is constitutionally prohibited. Privacy have to be balanced towards valid goals, challenge to constitutional necessities. The proportionality method evolved via the Supreme

⁶ Information Technology Act, 2000, sec 43A, India Code (2000).

⁷ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Ministry of Communications & Information Technology (Apr. 11, 2011).

⁸ *Puttaswamy*, (2017) 10 SCC 1. See also Supreme Court of India, Judgment in W.P. (C) No. 494 of 2012 (Aug. 24, 2017)

Court requires consideration of legality, legitimate motive, rational connection, necessity and safeguards against abuse.⁹

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

SCOPE AND APPLICATION

The DPDP Act regulates the processing of virtual personal statistics. It applies to processing within India wherein non-public facts is gathered in virtual form or gathered in non-virtual form and subsequently digitized. It may observe to processing outdoor India where such processing is attached with offering goods or services to Data Principals within India, challenge to the statutory framework.¹⁰

This territorial technique is giant due to the fact digital offerings often perform throughout countrywide borders. An Indian consumer may additionally use a overseas platform whose servers, employees, cloud providers and information processors are positioned in different jurisdictions.

DATA PRINCIPAL

The Act uses the time period “Data Principal” to describe the character to whom the private information relates. This terminology is conceptually crucial because it locations the person on the centre of the regulatory dating.

The Data Principal receives statutory rights concerning get entry to, correction, erasure, criticism redressal and nomination.¹¹

DATA FIDUCIARY

The “Data Fiduciary” is the entity that determines the reason and way of processing private information. This concept broadly resembles the controller concept discovered in different data safety frameworks.

⁹*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2018) 12 SCC 1. The proportionality approach requires, among other things, a legitimate objective, rational connection, necessity and safeguards against abuse.

¹⁰ Digital Personal Data Protection Act, 2023, sec 3, India Code (2023).

¹¹ *Id.* sec 11–14.

The difference among Data Principal and Data Fiduciary establishes an accountability relationship. The person materials or is associated with the statistics, at the same time as the Data Fiduciary determines how and why it's miles processed.

CONSENT AND LAWFUL PROCESSING

Consent is a relevant function of the DPDP Act. Section 6 calls for consent to be loose, unique, knowledgeable and unambiguous, related to a clean affirmative motion. A request for consent must be provided in clean and undeniable language.

This technique acknowledges that consent cannot meaningfully shield individuals if it's far hidden in prolonged or incomprehensible contractual language.

The DPDP Rules, 2025 toughen this requirement. Rule 3 calls for a Data Fiduciary's notice to be comprehensible independently of other statistics and to provide an itemized description of personal records and the functions for which its miles processed. The Rules additionally require information allowing Data Principals to withdraw consent and exercising their rights.¹²

This is a full-size compliance improvement because companies will need to rethink privacy notices, consent mechanisms, utility interfaces and contractual documentation.

However, consent has inherent boundaries. In many virtual relationships, people may additionally have little sensible bargaining strength. A customer may be not able to get entry to an important provider without agreeing to sizeable processing. Consent can consequently become formal in preference to sincerely voluntary.

The DPDP Act in part addresses this difficulty through “sure valid uses” below phase 7, which acknowledges circumstances in which processing might also occur without conventional consent.¹³ This displays the practical fact that each lawful processing operation cannot depend upon person consent.

The crucial project is consequently no longer truly acquiring consent but ensuring that processing is proportionate, transparent and linked to valid purpose.

¹² Digital Personal Data Protection Rules, 2025, r. 3. The final Rules require clear, independent and understandable notices and specify that notices should include an itemized description of personal data and the purposes of processing.

¹³ Digital Personal Data Protection Act, 2023, sec 7, India Code (2023).

OBLIGATIONS OF DATA FIDUCIARIES

Section 8 imposes several well-known duties on Data Fiduciaries. These consist of obligation for compliance, accuracy where facts is used for sure purposes, implementation of affordable protection safeguards, breach notification, deletion of personal statistics when retention is not essential and status quo of grievance-redressal mechanisms.¹⁴

The security duty is mainly essential because information protection can't be executed solely thru contractual consent. Organizations should hold technical and organizational safeguards designed to prevent unauthorized get admission to, disclosure, alteration or destruction.

The DPDP Rules, 2025 provide greater operational element concerning protection safeguards. The final Rules require suitable technical and organizational measures and prescribe a framework addressing matters which includes encryption, get admission to controls, logging, tracking, backup and different safety-associated safeguards.¹⁵

This represents an essential transition from a primarily principle-based statutory responsibility in the direction of a greater operational compliance framework.

Organizations have to consequently adopt a privateness-through-design approach. Data mapping, retention schedules, get right of entry to controls, incident reaction plans, vendor management, employee training and periodic security tests should grow to be quintessential elements of organizational compliance.

PERSONAL DATA BREACHES

Data breaches represent one of the main risks addressed via the DPDP framework.

A breach can disclose individuals to identification robbery, monetary fraud, account compromise, impersonation and different harms. The DPDP Act imposes responsibilities on Data Fiduciaries to notify the Board and affected Data Principals in the prescribed manner.¹⁶

The DPDP Rules provide more element regarding breach notification. This creates a extra established incident-reaction responsibility for agencies.

¹⁴ Id. sec 8

¹⁵ Digital Personal Data Protection Rules, 2025, rules concerning reasonable security safeguards. See Ministry of Electronics & Information Technology, *Digital Personal Data Protection Rules, 2025*.

¹⁶ Digital Personal Data Protection Act, 2023, sec 8, India Code (2023).

The transition is widespread while compared with the sooner framework underneath phase 43A of the IT Act, which focused mostly on negligence in preserving affordable safety practices. The DPDP framework locations breach control within a broader duty architecture.

Effective breach regulation nonetheless requires groups to have incident-response mechanisms earlier than a breach takes place. Compliance cannot realistically begin after an incident. Organizations need to keep documented methods for detection, containment, investigation, notification and remediation.

PROTECTION OF CHILDREN'S DATA

Children require unique protection because they may lack the adulthood to recognize the long-time period effects of statistics disclosure.

Section 9 establishes extra obligations concerning kid's personal information. It calls for verifiable parental consent and restricts positive varieties of processing concerning children.¹⁷

The Act prohibits processing probably to cause unfavorable results on the well-being of kids and imposes regulations concerning monitoring, behavioral monitoring and centered advertising directed at children, concern to the statutory framework.

The DPDP Rules, 2025 offer mechanisms for determining and verifying parental consent.¹⁸

This is an important place of regulation due to the fact children increasingly more have interaction with social media, gaming, instructional structures, streaming offerings and AI-powered applications.

Nevertheless, verification mechanisms create their very own privacy concerns. A machine designed to verify whether or not an individual is a discern may also itself require the gathering of extra non-public records. Consequently, child-protection mechanisms ought to follow facts minimization concepts and ought to no longer create unnecessary surveillance.

CROSS-BORDER DATA TRANSFERS

Modern virtual offerings often contain international data transfers. Cloud infrastructure, multinational businesses, price systems and software program-as-a-service platforms may additionally process Indian personal statistics outdoor India.

¹⁷ Id. sec 9.

¹⁸ Digital Personal Data Protection Rules, 2025, rules concerning verifiable consent for processing children's personal data. The Rules establish mechanisms for verification of parental consent.

Section 16 of the DPDP Act lets in the Central Government to limit transfers of private records out of doors India to special international locations or territories through notification.¹⁹

This is structurally extraordinary from a device that establishes a complete whitelist of approved nations.

The Indian technique gives the government extensive flexibility. It can probably facilitate global trade while maintaining the capability to limit transfers wherein vital.

At the equal time, agencies need predictability. International statistics transfers are regularly embedded into technological structure and business contracts. Sudden restrictions may additionally therefore generate widespread compliance costs.

India's pass-border records framework need to consequently searching for to balance national pursuits, person privacy, international change and interoperability with foreign records safety systems.

GOVERNMENTAL EXEMPTIONS AND THE RIGHT TO PRIVACY

One of the hugest areas for critical analysis issues exemptions.

Section 17 presents occasions in which exact provisions of the Act may not observe or may additionally practice otherwise. These consist of positive processing important for legal features, judicial or regulatory capabilities, prevention or detection of offences and other designated public-interest purposes.²⁰

Exemptions are necessary due to the fact governments have to be capable of perform valid public functions. Law enforcement, taxation, national protection, public health and judicial administration might also require processing of personal statistics.

Nevertheless, exemptions increase constitutional issues when they allow huge processing without equal safeguards.

The constitutional right to privateness does no longer create an absolute prohibition on state get right of entry to personal facts. Instead, kingdom action affecting privateness ought to satisfy constitutional standards consisting of legality, legitimate motive, necessity and

¹⁹ Digital Personal Data Protection Act, 2023, sec 16.

²⁰ Ministry of Electronics & Information Technology, *Data Protection Framework*, <https://www.meity.gov.in/data-protection-framework>.

proportionality. The Supreme Court's privateness jurisprudence consequently remains a critical interpretive protect.²¹

DATA PROTECTION BOARD OF INDIA

The Board is empowered to inquire into certain breaches, impose financial consequences and perform other features assigned by the Act.²²

The Central Government notified the status quo of the Board framework in November 2025 and unique that the Board would include 4 individuals²³

The advent of a specialized frame is a chief development in comparison with the sooner fragmented framework.

However, institutional layout is critical to regulatory credibility. A records protection authority ought to own ok technical understanding, criminal understanding, assets and procedural independence.

The Board will even face a big quantity of potential proceedings and compliance topics. Digital platforms may additionally process information concerning tens of millions of individuals, meaning that a regulatory machine have to be able to dealing with large-scale and technologically complicated disputes.

PENALTIES AND ENFORCEMENT

The DPDP Act adopts a substantial monetary penalty framework. The Schedule to the Act provides for penalties that can extend to hundreds of crores of rupees depending upon the nature of the breach.²⁴

The penalty structure is intended to create a meaningful incentive for organizational compliance.

The significant size of potential penalties reflects the economic importance of personal data and the potential scale of harm from systemic failures.

²¹ Supreme Court of India, *Judgment in W.P. (C) No. 494 of 2012*, Aug. 24, 2017, <https://www.sci.gov.in/>.

²² Digital Personal Data Protection Act, 2023, sec 18–26.

²³ Ministry of Electronics & Information Technology, Notification No. G.S.R. 845(E) (Nov. 13, 2025). The notification specifies that the Data Protection Board of India shall consist of four members.

²⁴ Digital Personal Data Protection Act, 2023, Schedule.

However, penalties alone cannot create effective data protection. A compliance framework should encourage organizations to prevent violations rather than simply punish them after the fact.

Factors such as the nature and gravity of the breach, affected individuals, and duration of the violation, security measures, mitigation efforts, recurrence and cooperation should be considered in enforcement.

The regulatory framework should therefore promote proportionality in penalties while maintaining meaningful deterrence.

DATA PROTECTION AND CORPORATE COMPLIANCE

The DPDP Act has vast results for company prison departments and compliance teams.

Organizations processing non-public data ought to set up a dependent compliance programme along with:

- Data inventory and mapping;
- Identification of Data Fiduciary and Data Processor relationships;
- Privacy notices;
- Consent control;
- Data retention schedules;
- Data deletion techniques;
- Vendor and processor due diligence;
- Data breach reaction plans;
- Security safeguards;
- Employee privateness schooling;
- Grievance mechanisms;
- Contractual records protection clauses;
- Cross-border records transfer assessments; and
- Periodic compliance audits.

Contracts with vendors need to mainly cope with approved processing, safety, confidentiality, breach notification, deletion, audit rights, subcontracting and help with Data Principal Requests.

This is especially important due to the fact an organization's records protection compliance is an increasing number of turning into a part of its broader corporate governance framework.

COMPARISON WITH THE CONSTITUTIONAL RIGHT TO PRIVACY

The DPDP Act have to not be regarded because the supply of the constitutional proper to privateness. The constitutional foundation existed earlier than the statute.

The significance of Puttaswamy is that privateness is an essential proper, even as the DPDP Act provides a statutory mechanism for regulating one crucial size of privacy: virtual non-public data.

The two frameworks therefore operate at different stages.

- The Constitution establishes a fundamental-rights framework that constrains state movement. The DPDP Act primarily establishes statutory responsibilities applicable to Data Fiduciaries and Data Principals.
- Judicial overview will continue to be important where statutory provisions or state processing practices have an effect on essential rights.

The principle of proportionality is in particular relevant. A statistics-processing degree affecting privateness should have a valid objective and should no longer impose a disproportionate burden on person rights.

CONCLUSION

The Digital Personal Data Protection Act, 2023 marks a sizeable level within the evolution of Indian statistics protection law. It moves India past the enormously fragmented framework related to section 43A of the Information Technology Act, 2000 and the SPDI Rules and creates a devoted statutory structure for digital private data.

The importance of the DPDP framework lies not simply within the introduction of new compliance necessities however inside the popularity that private statistics calls for based criminal governance. The Act locations obligations upon Data Fiduciaries, grants rights to Data Principals, establishes more desirable obligations for Significant Data Fiduciaries, presents unique protection for children, creates Consent Managers and establishes the Data Protection Board.

The Digital Personal Data Protection Rules, 2025 similarly rework statutory concepts into operational necessities. Their provisions concerning notices, consent management, protection

safeguards, breach notification and institutional mechanisms are especially crucial for implementation. The phased commencement method additionally recognizes the practical need for corporations to prepare for compliance.²⁵

Nevertheless, law alone cannot guarantee privacy. The effectiveness of the Indian framework will depend on implementation. Broad exemptions should be observed through appropriate safeguards. The Data Protection Board need to expand technical and criminal knowledge. Organizations ought to circulate beyond formal privacy rules towards authentic privacy-with the aid of-design practices. Individuals ought to take delivery of significant and reachable mechanisms for exercise their rights.

The constitutional jurisprudence of Puttaswamy offers the broader normative basis for those traits. Privacy is hooked up with dignity, autonomy and liberty, while facts protection provides mechanisms for protecting those interests in and an increasing number of virtual society.

India's venture is consequently to set up a machine in which innovation and facts-pushed economic interest can hold without treating private data as a vast industrial resource. A success records safety framework must facilitate lawful statistics use while stopping pointless, disproportionate and unauthorized processing.

The DPDP Act represents an essential basis for attaining that goal. Its final success, but, might be determined by using the best of its implementation, regulatory independence, technological capability, judicial interpretation and the willingness of public and personal establishments to treat privacy as a substantive governance responsibility in preference to simply a compliance formality.

²⁵ Ministry of Electronics & Information Technology, *Digital Personal Data Protection Rules, 2025* (Nov. 13, 2025). The Rules were notified with an eighteen-month phased implementation mechanism.