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

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: STRIKING A BALANCE BETWEEN INNOVATION, COMPLIANCE AND PRIVACY.

~Shubha Sree H

ABSTRACT

The Digital Personal Data Protection Act, 2023 marks a significant achievement for the governance of India's digital environment by developing an integrated strategy that both protects data privacy and encourages innovation and economic growth. The purpose of this paper is to assess the Act through a critical analysis of three of its key functions: consent-based processing of personal data, rights of the individual whose personal data has been used, and how organizations deal with their obligations to comply with the Act and the operations of the Data Protection Board of India.

Keywords: Digital environment, Data privacy, Innovation.

INTRODUCTION

The Digital Personal Data Protection Act, 2023 (DPDP Act) was enacted on August 11, 2023 in India.[1] This represents a significant step forward in the development of cyber-constitutional law in India because it will modify the existing infringements under the Information Technology Act, 2000.[2]The DPDP Act, represents India's first significant legislative effort to establish the Constitutional Right to Artificial Intelligence and Data Privacy. India is both an emerging technology-based country and home to one of the world's largest digital economies, and so very clearly faces the daunting task of establishing a legislative framework that allows

[1] Press Release, Press Info. Bureau, Govt of India, *Digital Personal Data Protection Rules 2025 Notified* (Nov. 17, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190655&reg=48&lang=2.

[2] Information Technology Act, No. 21 of 2000.

for the optimal protection of the personal data of over 900 million people while still permitting commercial enterprises to innovate and engineer artificial intelligence, as well as augment digital infrastructure.

The DPDP Act will work to resolve this conflict by utilizing a more concise & principle-based architecture in place of the overly complex and rule-heavy architecture commonly found within Western frameworks, like what is available within the General Data Protection Regulation (GDPR). This analysis will explore the extent to which the Indian Regulatory System is successfully achieving a balance between the sometimes-conflicting requirements of the DPDP rules, once they are put into effect.

BACKGROUND

The rapidly growing sector of data collection in India has existed for two decades with the existing legal framework which regulates the usage of such data. The governing legal framework of this field of law consists of the Information Technology Act of 2000 and its section 43A,[3] as well as Information Technology (Information Security Practices and Sensitive Personal Data) Rules of 2011. Nevertheless, this legal framework can be considered inadequate and has covered a limited number of forms of sensitive personal data, such as passwords, financial data and diseases, which is the basis of addressing these issues through civil claim for the damages caused,[4] not compensation for the loss of sensitive personal data. It should be also mentioned that it is rather regrettable that the existing law does not regulate the question of whether the state has the right to gather data from us.

But it should be mentioned that structural reforms in the system became necessary after the judgment by a nine-judge bench of the Supreme Court of India in a case known as Justice K. S. Puttaswamy v. Union of India in August 2017[5]. The Supreme Court ruled that the right to privacy is an essential component of Article 21[6] of the Indian Constitution, which provides that people of India have the right to life and personal liberty. It follows from the above that there is a right to make sure that one's informational privacy is preserved as the right to informational privacy is associated with one's dignity and autonomy. Additionally, it is worth mentioning

[3] Information Technology Act, No. 21 of 2000, § 43A.
[4] Chukwuka Elenda et. al., *Legal implications for clinicians in cybersecurity incidents: A review* (Sept. 27, 2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC11441973/.
[5] *Justice K.S. Puttaswamy (Retd.) v. Union of Indi*a, (2017) 10 SCC 1.
[6] INDIA CONST. art. 21.

that violations of the right to informational privacy by any entity should satisfy certain constitutional requirements.

When the landmark Puttaswamy case was decided, it made abundantly clear that there was an urgent need for specific data laws in India as the country's use of the internet grew rapidly. In addition to the widespread availability of low-cost mobile data, the launch of the Unified Payments Interface (UPI) across India helped generate hundreds of millions of new users of the internet who created their own profiles every day online, resulting in an explosion of digital content.[7] Five years of rigorous public and legislative debate were required to move from the first draft prepared by the B.N. Srikrishna expert group back in 2018 to the formal passage of legislation in 2023.[8] More than one version of the bill had to be passed before finally passing this complete change from the prior 2019 version of the bill, as well as developing a legal structure for data localization. Through the Supreme Court's historic recognition of the need for and creation of an entirely new way of providing a legal basis for data use, this final law will be "digital sovereignty" in the age of the internet.

KEY FEATURES OF THE ACT

The DPDP Act is based on a single classification of Digital Personal Data instead of using multiple tiers of classification like sensitive or critical personal data. The law applies to any kind of data that exists in either an analog or digital form, provided that it has been converted into a digital form after the date of collection (e.g., paper documents), and that allows for the identification of one specific person using that data.

“There are three primary participants in the DPDP Act ecosystem:

1) Data Principal - An individual for whom data is being processed;

2) Data Fiduciary - An individual or entity that determines how and why personal data will be processed; and

3) Data Processor - An individual or entity that processes personal data on behalf of a Data Fiduciary.”[9]

---

[7] Aishvarya Jain, *India crosses 107 crores Internet Connections, 75 Crore Daily UPI Payments, NDTV* (June 30, 2026), https://www.ndtv.com/india-news/india-crosses-107-crore-internet-connections-75-crore-daily-upi-payments-11706252.

[8] PRS Legislative Research, *Draft Personal Data Protection Bill, 2018*, https://prsindia.org/billtrack/draft-personal-data-protection-bill-2018.

[9] Digital Personal Data Protection Rules 2025 Notified, supra note 1.

THE ROLE OF CONSENT AND NOTICE

Section 4[10] of the Data Protection Act defines consent as a lawful condition to process personal data if there is an explanation notice accompanying unambiguous, informed, non-coerced and clear directives of how the data processor may process that person's data. In order to ensure the notice is in a form that all people in the various languages throughout the country can understand, all notices must be in English and in each of the 22 languages identified in the 8th Schedule of the Constitution.

Consent managers

A consent manager is a new type of organization established by the Data Protection Act that is registered and accountable to the Data Protection Board of India. The consent manager is an individual's digital intermediary and provides individuals with the ability to give, change, review and revoke their consent via digital means**.**[11]

D.P.B.I. (The People's Data Protection Bureau of India)

The Data Protection Bureau of India (DPBI), as established by the Act, acts on behalf of and on behalf of the people of India. The DPBI does not simply "monitor" data breaches, but also reviews reports of data breaches issued by data solicitations from third parties and, where appropriate, investigates the parties who violate the Act.[12]

The Puttaswamy case established the foundational right to privacy. With this in mind, the DPDP Act now implements this constitutional directive by giving citizens enforceable rights against third parties with regard to their digital identities. Previously, citizens were regarded only as users or consumers of their data; however, now they will be viewed as Data Principals, meaning that they own their data.

The rights granted to citizens through this framework are:

Right of Access: The data principal is entitled to receive a concise account of the activities relating to the processing of the personal data. The data principal also has the authority to ask

[10] Digital Personal Data Protection Act, No. 22 of 2023, § 4.

[11] Nandan Pendsey, Arun Babu & Zahra Vakil, *Consent Managers under India's DPDP Act and DPDP Rules*, AZB & Partners (Jan. 13, 2026), https://www.azbpartners.com/bank/consent-managers-under-indias-dpdp-act-and-dpdp-rules/

[12] Prashant Mali, *Data Protection Board of India: Powers, Procedures & Adjudication*, DPDPA.com (Feb. 1, 2026), https://www.dpdpa.com/blogs/data_protection_board_india_dpbi_powers_procedures.html.

the names of the data fiduciaries/data processors who have access to his personal data along with an explanation of the manner in which the personal data is being processed.

Right of Correction and Deletion: The data principal has the right to get any incorrect or incomplete or misleading personal information regarding him corrected or completed by the data fiduciary or deleted after he has utilized the personal data of the data principal or when he withdraws his consent for processing.

Right to a Grievance Redressal: Prior to making a complaint to any regulator, the data principal has the right to make use of the process of grievance redressal instituted by the data fiduciary.

The Right to Nominate Another Person: In relation to addressing some of the dilemmas of the digital age, an individual may designate another person to have the rights to manage, alter, and delete their digital personal information in the event of their death or incapacity. The use of consumer digital responsibility will be a product of the implementation of these data principal rights into the digital platform of consumers.

COMPLIANCE OBLIGATIONS

When a company operates in a framework where there is generally no regulation; however, they must adhere to mandatory regulations with strict liability. Companies face costs that are both operational and financial as they transition into compliance. The DPDP establishes a multi-layered compliance model, where the most stringent compliance requirements are assigned to SDFs (Service Data Hosts), based on factors including size, risk to DP's rights, and sovereignty implications.[13]

- **Basic Institutional Compliance**
  Regular Data Fiduciaries need to implement adequate technical and organizational safeguards for the purposes of establishing appropriate traceability.
- **Limitations on Purpose and Storage:** Fiduciaries must remove personal information when it is no longer necessary to achieve its intended purpose to collect the data or when a user withdraws their consent. The DPDP Rules specify that an objective basis

[13] Anahad Narain, *Significant Stakes: DPDP Compliance for Large Enterprises* (July 4, 2025), https://www.consent.in/blog/significant-data-fiduciary.

will be used to define fulfillment of the intended purpose of collected personal data. As per the DPDP Rules if a user has not interacted with the service for a period of time, the intended purpose of the personal data collection will have been achieved.

- **Data Accuracy:** Fiduciaries are expected to ensure that the accuracy of any personal data that will impact any Data Principal or will be shared with any third party.
- **Breach Notifications**: If a data breach should occur, Section 8(6) of the Data Protection [14]Bill removes all discretion of a fiduciary regarding notification; therefore, the Fiduciary would be required to notify the Data Protection Board of India (DPBI) and all Data Principals that have been impacted by the breach.

CRITICAL ANALYSIS

The Data Protection Development Program (DPDP) indicates many inconsistencies, gaps, and significant social/legal conflict within the regulatory structure. Though successful in moving away from excessive bureaucracy found within European data regulations, the DPDP contains elements that may jeopardize citizen privacy rights as well as corporate efficiency. Section 17(2) of the DPDP,[15] which permits any central government agency or agency of the state to be granted an unlimited exemption from being subject to the Data Protection Act based upon broad grounds of either national sovereignty, public order, foreign affairs, or state security, is the most contentious issue in regard to the entire DPDP legal framework. While a private E-commerce business may receive heavy penalties for any accidental breach of personal information within their business, all state entities that manage personal information on their citizens have complete legal immunity.

- Right to Information (RTI) Dilution.

Section 44 of the DPDP Act[16] modifies Section 8(1)(j) of the RTI Act, 2005[17] and is forever changed. Under RTI law, if a public body has personal information concerning someone, it may choose not to release that information if the release would not relate to providing any publicly related services/activities and would result in the release of personal information which could reasonably be expected to cause an unsolicited breach of privacy to the individual.

[14] Digital Personal Data Protection Act, No. 22 of 2023, § 8(6).
[15] Digital Personal Data Protection Act, No. 22 of 2023, § 17(2).
[16] Digital Personal Data Protection Act, No. 22 of 2023, § 44.
[17] Right to Information Act, No. 22 of 2005, § 8(1)(j).

Even in that case, the public body could still disclose the information if it served a greater public good.

However, the way that section is written under the new DPDP system, absolutely no balancing test can be used to determine whether a person's personal information will be released due to the greater public good. Academics and anti-corruption activists believe that this limitation on RTI amounts to a serious hindrance to transparency because: It is the case that public servants have the ability to refuse a request from the public concerning asset declarations, educational qualifications, work performance records, or appointments to public office due to concerns about protecting confidential information. Although the law is meant to allow access and transparency for individuals, the law has caused governments to use it as a way of avoiding providing access to or being transparent about information.

- The Friction of Complying with Child Data

Section 9 of the Act[18] has created an extremely rigorous process for managing the personal information of children. As a result, it has prohibited the use of profiling; the use of behavioral tracking; and the use of marketing directed at individuals under the age of eighteen (18) years. Additionally, each data fiduciary is required to have parental consent prior to processing a child's personal data. While similar sovereign immunity provisions exist in other nations' legal frameworks for privacy issues (internationally), India lacks judicial mechanisms, external audit processes or the requirement of a balancing of competing interests.

- Dark Patterns: Uncertainties in Implementation

Despite the DPDP rules clearly banning the use of dark patterns user interfaces aimed at manipulating users and getting access to additional information from them it is quite hard to draw a line between aggressive online advertising and illegal manipulation. It is especially difficult for young companies and middle businesses that constantly face uncertainties in developing user interfaces due to possible sanctions for unclear consent forms.

CONCLUSION

[18] Digital Personal Data Protection Act, No. 22 of 2023, § 9.

The DPDPA is a leading-edge initiative created by India in relation to its digital economy. The Act has provided a more streamlined principles-based framework as opposed to the bureaucratic framework of the EU's GDPR, allowing the act to provide continued business agility; facilitate cross-border data transfers; and encourage further development of Artificial Intelligence technologies.

However, the future of the act will depend on its implementation by the Data Protection Board of India in a manner that is transparent, providing consumers with a right to privacy and protecting business interest. If the act is implemented in this way, then abuse of the exemptions given to the Government will be avoided and will not create an increasing administrative burden for businesses due to inconsistent application of compliance measures; however, public data will still not be better protected.