



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 THE DIGITAL AGE: A CRITICAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

~ Gagandeep Kaur

Abstract

The Digital Personal Data Protection Act, 2023 marks India's first comprehensive law on the processing of digital personal data. Enacted after the Supreme Court recognised the right to privacy as a fundamental right in the Puttaswamy case, the Act seeks to balance individual privacy with the needs of a growing digital economy. It introduces a consent-based framework, defines the roles of Data Principals and Data Fiduciaries, grants limited rights to individuals, and creates the Data Protection Board of India for enforcement. This article critically examines the key provisions of the Act, including consent requirements, fiduciary obligations, cross-border data transfers, and wide government exemptions. The law is a significant step forward, however, it has notable limitations in rights protection and institutional independence. The article compares it briefly with the GDPR and suggests reforms to strengthen privacy safeguards in the digital age.

Keywords: Digital Personal Data Protection Act, 2023, Right to Privacy, Informational autonomy

1. INTRODUCTION

The rapid expansion of digital technologies in India has transformed the way personal data is collected, stored, and used. From Aadhaar-enabled services and unified payment systems to social media platforms and artificial intelligence applications, vast amounts of personal information are processed daily. While these developments have improved efficiency and convenience, they have also raised serious concerns about privacy, data breaches, profiling, and unauthorised surveillance. The constitutional foundation for addressing these concerns was firmly established in *Justice K.S. Puttaswamy (Retd.) v. Union of India*¹, where the Supreme Court recognised the right to privacy as a fundamental right under Article 21 of the Constitution. The judgment specifically highlighted the need for a robust data protection framework to safeguard informational privacy in the digital age.

¹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

In response, the Digital Personal Data Protection Act, 2023 was enacted after years of deliberation, including the recommendations of the Justice B.N. Srikrishna Committee and several draft bills. The Act aims to regulate the processing of digital personal data while balancing individual rights with the legitimate needs of the state and the digital economy. This article critically examines the key provisions of the DPDP Act, 2023. It argues that although the law represents an important step forward, certain structural weaknesses, particularly broad government exemptions and limited individual rights undermine its effectiveness. The article is structured to analyse the scope of the Act, its core obligations and rights, enforcement mechanisms, and areas requiring reform.

2. OVERVIEW OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 was enacted with the primary objective of regulating the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such data for lawful purposes.² The Act seeks to create a balance between individual privacy and the requirements of a growing digital economy, while also addressing concerns related to data security and accountability.³

In terms of scope, the Act applies to the processing of digital personal data within the territory of India. It also has extraterritorial application where personal data is processed outside India in connection with any activity related to the offering of goods or services to individuals located in India.⁴ However, the Act does not apply to personal data processed for purely personal or domestic purposes, or to data that is made publicly available.⁵

The Act introduces several key definitions that form the foundation of its regulatory framework. A Data Principal refers to the individual to whom the personal data relates. In the case of children or persons with disability, it includes their parents or lawful guardians.⁶ A Data Fiduciary is any person or entity that determines the purpose and means of processing personal data, either alone or in conjunction with others.⁷ A Data Processor, on the other hand, processes personal data on behalf of a Data Fiduciary. Personal data is defined broadly as any data about an individual who is identifiable by or in relation to such data.⁸

An important feature of the Act is the category of Significant Data Fiduciaries. The Central Government may notify certain Data Fiduciaries as Significant Data Fiduciaries based on factors such as the volume and

² Digital Personal Data Protection Act, 2023, No. 22 of 2023, Preamble.

³ Dr. Pradip Kumar Kashyap, *Digital Personal Data Protection Act, 2023: A New Light into the Data Protection and Privacy Law in India*, 2 ICREP J. Interdisciplinary Stud. Iss. 1 (2023).

⁴ Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 3(a)–(b).

⁵ *Id.* § 3(c).

⁶ *Id.* § 2(j).

⁷ *Id.* § 2(i).

⁸ Anurag Sourot & Deepali Kushwaha, *Critical Analysis of the Digital Personal Data Protection Act, 2023*, 7 Indian J. L. & Legal Res. Iss. II, 7356, 7359-7360 (2025).

sensitivity of personal data processed, the risk of harm to Data Principals, and potential impact on the sovereignty and integrity of India.⁹ These entities are subject to additional obligations, including the appointment of a Data Protection Officer and the conduct of data protection impact assessments.¹⁰ Overall, the Act establishes a structured framework that clearly identifies the roles and responsibilities of different stakeholders involved in the processing of personal data.

3. LAWFUL PROCESSING OF PERSONAL DATA

The Digital Personal Data Protection Act, 2023 places consent at the centre of lawful data processing. As a general rule, a Data Fiduciary may process the personal data of a Data Principal only after obtaining consent for a specific purpose.¹¹ This consent-based approach seeks to give individuals greater control over their personal information in the digital environment.

For consent to be valid under the Act, it must be free, specific, informed, unconditional and unambiguous. It must also be given through a clear affirmative action. The Data Principal has the right to withdraw consent at any time, and the process of withdrawal must be as easy as the process of giving consent.¹² Once consent is withdrawn, the Data Fiduciary is required to cease processing the personal data unless another lawful ground applies.¹³

Before or at the time of requesting consent, the Data Fiduciary must provide a clear and easily understandable notice to the Data Principal. This notice should inform the individual about the personal data to be collected and the purpose of its processing. The notice must also explain the rights available to the Data Principal and the process for making complaints. Where possible, the notice should be made available in English or any language specified in the Eighth Schedule of the Constitution.

The Act also permits processing of personal data without consent in certain specified situations. These include cases where the Data Principal has voluntarily provided the data for a particular purpose, processing necessary for the performance of state functions such as the provision of benefits or services, compliance with legal obligations, medical emergencies, and employment-related purposes.¹⁴

⁹ Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 10(1); Anurag Sourot & Deepali Kushwaha, *Critical Analysis of the Digital Personal Data Protection Act, 2023*, 7 Indian J. L. & Legal Res. Iss. II, 7356, 7364 (2025).

¹⁰ Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 10(2).

¹¹ *Id.* § 4.

¹² *Id.* § 6.

¹³ Shubham Saurabh, *The Digital Personal Data Protection Act of 2023: Strengthening Privacy in the Digital Age*, 4 Indian J. Integrated Rsch. L. Iss. V, 1183, 1187-1188 (2024).

¹⁴ Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 7.

While the emphasis on consent is a positive feature, the wide range of legitimate uses particularly those available to the State raises concerns. The absence of strict necessity and proportionality requirements for these exceptions may dilute the protective intent of the consent framework and tilt the balance in favour of organisational and governmental interests.

4. OBLIGATIONS OF DATA FIDUCIARIES

The Digital Personal Data Protection Act, 2023 imposes a range of obligations on Data Fiduciaries to ensure responsible processing of personal data. These duties form the core of the compliance framework under the Act.

General Obligations

Every Data Fiduciary is required to process personal data only for the purpose for which consent has been obtained or for a legitimate use permitted under the Act. The Data Fiduciary must ensure that the personal data is complete, accurate and consistent, especially where it is likely to be used for decisions affecting the Data Principal.¹⁵ Personal data should not be retained for longer than necessary to fulfil the stated purpose, and appropriate measures must be taken to erase the data once the purpose is served.¹⁶

Security Safeguards and Breach Notification

Data Fiduciaries are under a duty to implement reasonable security safeguards to prevent personal data breaches. In the event of a breach, the Data Fiduciary must notify the Data Protection Board of India and the affected Data Principals in the manner prescribed. Failure to maintain adequate security measures can attract significant financial penalties.¹⁷

Special Provisions for Children's Data

The Act provides heightened protection for the personal data of children. A Data Fiduciary must obtain verifiable consent from the parent or lawful guardian before processing a child's data. It is also prohibited from undertaking tracking, behavioural monitoring, or targeted advertising directed at children. These restrictions aim to protect minors from exploitative data practices.¹⁸

Additional Duties of Significant Data Fiduciaries

Significant Data Fiduciaries are subject to extra compliance requirements. These include the appointment of a Data Protection Officer, the conduct of data protection impact assessments, and independent audits of their data

¹⁵ *Id.* § 8(3).

¹⁶ Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 8(7); Prabhash Dalei, *The Digital Personal Data Protection Act, 2023: A Legal Analysis in Light of Global Data Protection Standards*, 11 Int'l J. L. 127, 128 (2025).

¹⁷ Digital Personal Data Protection Act, 2023, No. 22 of 2023, §§ 8(5), 8(6).

¹⁸ *Id.* § 9; Prabhash Dalei, *The Digital Personal Data Protection Act, 2023: A Legal Analysis in Light of Global Data Protection Standards*, 11 Int'l J. L. 127, 128-129 (2025).

processing activities. These additional obligations reflect the higher risk associated with the volume or nature of data they handle.

5. RIGHTS OF DATA PRINCIPALS

The Digital Personal Data Protection Act, 2023 confers certain rights on Data Principals to enable them to exercise control over their personal data. These rights form an important part of the individual empowerment framework under the Act.¹⁹

Right to Access Information

A Data Principal has the right to obtain confirmation from the Data Fiduciary as to whether their personal data is being processed. They may also request a summary of the personal data being processed and information about the processing activities, including the identities of other Data Fiduciaries and Data Processors with whom the data has been shared.²⁰

Right to Correction and Erasure

The Data Principal is entitled to request correction of inaccurate or misleading personal data. They may also seek completion of incomplete data and updating of information that is out of date. In addition, the Data Principal has the right to request erasure of personal data that is no longer necessary for the purpose for which it was processed, or where consent has been withdrawn.

Right to Grievance Redressal

Every Data Principal has the right to an readily available means of registering a grievance with the Data Fiduciary. If the grievance is not resolved satisfactorily, the Data Principal may approach the Data Protection Board of India for further redressal.

Right to Nominate

The Act introduces a unique right allowing a Data Principal to nominate any other individual who may exercise their rights in the event of the Data Principal's death or incapacity. This provision addresses the issue of digital succession and ensures continuity in the exercise of data rights.

Despite these protections, the Act does not expressly provide for certain rights commonly found in other data protection regimes, such as the right to data portability or a clear right to object to processing. The absence of specific safeguards against solely automated decision-making also limits the scope of individual control. These

¹⁹ Digital Personal Data Protection Act, 2023, No. 22 of 2023, §§ 11–14.

²⁰ Shubham Saurabh, *The Digital Personal Data Protection Act of 2023: Strengthening Privacy in the Digital Age*, 4 Indian J. Integrated Rsch. L. Iss. V, 1183, 1189-1191 (2024).

gaps reduce the overall strength of the rights framework when compared to more comprehensive international standards.²¹

6. CROSS-BORDER TRANSFERS AND GOVERNMENT EXEMPTIONS

The Digital Personal Data Protection Act, 2023 contains important provisions on the transfer of personal data outside India and grants wide exemptions to the government. These aspects have generated significant debate regarding the balance between privacy, national interest, and accountability.²² The Act adopts a relatively permissive approach to cross-border data transfers. Personal data may be transferred to any country or territory outside India, except to those specifically restricted by the Central Government through notification. This negative-list model allows free flow of data by default and is intended to support India's digital economy and global business operations. However, the absence of clear criteria for placing countries on the restricted list leaves considerable discretion with the executive.

Section 17 of the Act empowers the Central Government to exempt any instrumentality of the State from the application of most provisions of the law. Such exemptions may be granted in the interests of the sovereignty and integrity of India, security of the State, public order, or friendly relations with foreign States. The government may also exempt certain Data Fiduciaries or classes of Data Fiduciaries from specific obligations for a limited period. These powers are wide and are not subject to detailed procedural safeguards under the Act.

The DPDP Act amends the Right to Information Act, 2005 by removing the public interest override that previously allowed disclosure of personal information in certain cases.²³ This change has raised concerns that it may reduce transparency and limit citizens' access to information held by public authorities. The combination of broad state exemptions and limited oversight mechanisms has led to criticism that the Act does not adequately protect individuals against potential surveillance or excessive data collection by government agencies. The lack of independent approval or proportionality requirements for exemptions remains a significant point of concern.

7. ENFORCEMENT MECHANISM

The Digital Personal Data Protection Act, 2023 establishes a dedicated institutional framework for the enforcement of its provisions. The effectiveness of the law largely depends on the functioning of this enforcement mechanism.²⁴

²¹ Rudraksh Lakra, Medha Kolanu & Abhijeet Shrivastava, *Data, Control, and Power: Decoding India's Digital Personal Data Protection Act, 2023*, 6 Glob. Priv. L. Rev. 4 (2025).

²² Digital Personal Data Protection Act, 2023, No. 22 of 2023, §§ 16–17.

²³ *Id.* § 44(3).

²⁴ *Id.* §§ 18–33.

The Act provides for the establishment of the Data Protection Board of India as the primary adjudicatory body. The Board is responsible for receiving complaints, conducting inquiries into personal data breaches, and imposing penalties for non-compliance. It has the power to direct Data Fiduciaries to take corrective measures and to issue orders for the payment of penalties. The Board functions as a digital office and is expected to adopt online procedures for the efficient disposal of cases.

A significant concern relates to the independence of the Board. The members of the Data Protection Board are appointed by the Central Government. Critics argue that this arrangement may affect the Board's ability to function independently, particularly when inquiries involve government agencies or powerful Data Fiduciaries. Questions have also been raised about the Board's capacity to handle a large volume of complaints and its technical expertise in complex data protection matters.²⁵

The Act provides for substantial financial penalties to deter non-compliance. Failure to take reasonable security safeguards can attract a penalty of up to ₹250 crore.²⁶ Failure to notify a personal data breach or non-compliance with provisions relating to children's data can lead to penalties of up to ₹200 crore. Other violations attract lower but still significant penalties. The high quantum of fines is intended to ensure serious compliance by Data Fiduciaries.

Orders passed by the Data Protection Board can be appealed before the Telecom Disputes Settlement and Appellate Tribunal. The Act also encourages alternative dispute resolution mechanisms and allows for voluntary undertakings by Data Fiduciaries to address non-compliance without prolonged proceedings. Overall, while the enforcement structure is clearly defined, its success will depend on institutional independence, adequate resources, and consistent application of the law.

8. CRITICAL EVALUATION

The Digital Personal Data Protection Act, 2023 represents a significant milestone in India's legal framework for data protection. However, a balanced assessment requires careful examination of both its positive features and its structural limitations.

Strengths of the DPDP Act

The Act deserves credit for establishing India's first comprehensive cross-sectoral data protection regime. It clearly recognises the importance of consent and places specific obligations on Data Fiduciaries, thereby creating a baseline of accountability that was previously missing under the limited provisions of the

²⁵ Teesha & Dhawal Shankar Srivastava, *Data Anonymisation, the Right to Explanation, and the Architecture of Accountability Under the Digital Personal Data Protection Act*, 1 HILSR L. Rev. 91 (2025).

²⁶ Digital Personal Data Protection Act, 2023, No. 22 of 2023, Schedule.

Information Technology Act, 2000.²⁷ The introduction of rights such as access, correction, erasure, and nomination gives individuals a degree of control over their personal data. The penalty structure, with fines going up to ₹250 crore, provides a strong financial deterrent against serious non-compliance. In addition, the relatively flexible approach to cross-border data transfers is designed to support India's digital economy and global service industry. The special protections for children's data further demonstrate an awareness of vulnerable groups.

Major Weaknesses and Criticisms

Despite these strengths, the Act has attracted substantial criticism. One of the most serious concerns is the wide range of exemptions available to the government under Section 17. These exemptions can be invoked on broad grounds such as national security and public order, without adequate procedural safeguards or independent oversight. This raises the risk of excessive state surveillance and weakens the protective purpose of the law. The rights granted to Data Principals are also limited when compared to international standards. The absence of a right to data portability and clear safeguards against automated decision-making reduces individual autonomy.²⁸ Further, the Data Protection Board of India is appointed entirely by the Central Government, which raises legitimate questions about its institutional independence, especially in cases involving state agencies. The removal of the public interest override from the Right to Information Act has also been viewed as a setback for transparency.²⁹

Comparative Analysis with the GDPR

A comparison with the European Union's General Data Protection Regulation (GDPR) highlights several differences. The GDPR provides a wider set of rights, including data portability and the right to object to processing, and subjects public authorities to stronger proportionality requirements.³⁰ It also establishes independent supervisory authorities with significant autonomy. In contrast, the DPDP Act adopts a more flexible and state-friendly model. While the GDPR follows a whitelist approach to cross-border transfers based on adequacy decisions, the Indian law uses a negative-list system that permits transfers by default. These differences reflect distinct policy priorities: the GDPR places stronger emphasis on individual rights, whereas the DPDP Act seeks to balance privacy with administrative convenience and economic growth.

²⁷ The Information Technology Act, No. 21 of 2000.

²⁸ Mamtaben Danabhai Patel, *Critical analysis of Digital Personal Data Protection Act, 2023: Safeguarding Privacy in the Digital Age*, 11 Int'l J. Res. All Subjects Multi Languages no. 8, 37, 40 (2023).

²⁹ Chetankumar T. M. & Rajendra Kumar Hittanagi, *An Analysis of Digital Personal Data Protection Act, 2023 and Intellectual Property Rights*, 13 Int'l J. Creative Rsch. Thoughts no. 1, h784 (2025).

³⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

In conclusion, the DPDP Act is an important first step towards a structured data protection regime in India. It fills a long-standing legislative gap and introduces essential concepts of consent, accountability, and enforcement. At the same time, its broad state exemptions, limited rights framework, and questions surrounding institutional independence prevent it from fully realising the constitutional vision of privacy laid down in the Puttaswamy judgment. Strengthening these areas will be essential if the law is to provide meaningful protection in the digital age.

9. RECOMMENDATIONS AND CONCLUSION

The Digital Personal Data Protection Act, 2023 affects individuals, businesses, and the State differently. While it offers citizens basic control over their data, organisations face new compliance responsibilities, and government agencies retain significant operational flexibility. To strengthen the law, the steps that should be taken include, to narrow the scope of government exemptions and introduce necessity and proportionality safeguards, enhance the institutional independence of the Data Protection Board of India, expand individual rights to include data portability and clearer protection against automated decision-making, restore a balanced public interest override in the Right to Information framework. The DPDP Act is a necessary and welcome foundation for data protection in India. However, its long-term success will depend on addressing existing gaps and ensuring that the right to privacy remains central in the digital age. Meaningful reform and effective implementation will determine whether the law truly fulfils the constitutional promise of informational privacy.