eISSN 3049-2610
Research Stream
A Bi-Annual, Open Access Pear Reviewed International Journal
Volume 03, Issue 01, March 2026

Data Protection on Paper: Implementation and Challenges of India's Digital Personal Data Protection Act , 2023

Vinod Kuma Verma[1]
[1]Assistant Professor V.S.S.D. College, Kanpur, Uttar Pradesh
Received: 20 March 2026 Accepted & Reviewed: 25 March 2026, Published: 31 March 2026

Abstract

The Digital Personal Data Protection Act, 2023 (DPDP Act) is the first comprehensive data protection law in India that creates a framework for the processing of digital personal data while attempting to balance individuals' privacy rights and legitimate business interests. However, moving from legislative intent to actual implementation presents enormous challenges that threaten the practical effectiveness of the DPDP Act. This paper critically assesses the implementation challenges associated with the DPDP Act by reviewing its avenues for enforcement, business compliance burden, and structural features. Our analysis surfaces five main issues: the centralised enforcement structure yielding an "enforcement deficit," disproportionate compliance burdens placed upon Micro, Small and Medium Enterprises (MSMEs), multi-layered consent management, resulting in "consent fatigue," regulatory uncertainty in cross-border data transfers, and congruence with existing laws. Through an assessment of academic analyses, industry reports, and comparative jurisprudence, we conclude that while the DPDP Act offers important principles of privacy, the implementation framework requires significant improvements regarding its ability to achieve its stated purpose. We provide specific recommendations regarding these implementation issues by way of decentralised enforcement, tiered compliance obligations, and improved regulatory guidance to facilitate compliance.
Keywords: Data Protection, DPDP Act 2023, Implementation Challenges, Enforcement Deficit, Digital Privacy, India Data Protection Board, Regulatory Compliance

Introduction

The ratification of India’s Digital Personal Data Protection Act, 2023 marks a pivotal moment in the context of the country’s data governance. After years of discussion and numerous incarnations of legislative proposals, India has finally achieved status as a country with a comprehensive data protection law. Enacted by the presidential assent on August 11, 2023, the Act aims to enable responsible processing of digital personal data and accountable data use while recognizing rights of individuals and lawful processing for business needs. However, the path from enactment to implementation has uncovered serious structural and operational challenges that may undermine the effectiveness of the law. Unlike the European Union’s General Data Protection Regulation (GDPR), which had established substantial preparatory stages and pilot implementations, of which the timeline of the DPDP Act is condensed with very little instruction to guide the work of stakeholders implementing compliance with the legislative framework. Additionally, the implementation process of the DPDP Act is compared to the unique economic landscape of India with a variety of large and small businesses, each facing different challenges to compliance. This paper examines the critical implementation challenges facing the DPDP Act through a comprehensive analysis of its enforcement architecture, compliance framework, and practical implications for various stakeholder groups. The research is grounded in the premise that effective data protection legislation requires not only sound legal principles but also viable implementation mechanisms that can be practically executed across India’s complex digital ecosystem.

II. Literature Review

eISSN 3049-2610
Research Stream
A Bi-Annual, Open Access Pear Reviewed International Journal
Volume 03, Issue 01, March 2026

2.1 Evolution of India's Data Protection Framework

The DPDP Act came about after a long drawn-out legislative process that started with the Justice B.N. Srikrishna Committee Report in 2018. The Act is the fourth attempt to establish data protection law, following the Personal Data Protection Bill, 2019 and subsequent drafts of the bill that were withdrawn. Scholarly scrutiny has suggested that while the lengthy time frame created an opportunity to engage with stakeholders, it also engendered regulatory uncertainty that has complicated implementation.

Commentators from academia have commented that the Act is a departure from comprehensive regulations like the GDPR, and a simpler approach to digital personal data. While that may be a positive step, the simplification may also create implementation gaps especially with respect to regulatory responsibilities and compliance requirements.

2.2 Comparative Analysis with Global Frameworks

Research comparing the DPDP Act with international data protection standards reveals both alignments and significant divergences. Unlike the GDPR's emphasis on multiple lawful bases for processing, the DPDP Act relies heavily on consent as the primary legal basis, creating implementation challenges around consent management and user experience.

The enforcement architecture under the DPDP Act has been particularly scrutinized in comparative literature. Studies examining the EU's decentralized enforcement model through Data Protection Authorities highlight potential benefits of localized oversight that the DPDP Act's centralized approach may not achieve.

III. Implementation Challenges

3.1 The Enforcement Deficit: Structural Limitations of Centralized Oversight

The DPDP Act provides for a centralized mechanism of enforcement through the Data Protection Board of India (DPB), which is the exclusive authority for investigating violations, adjudicating complaints, and imposing penalties. However, this centralization invokes what some legal scholars have called an "enforcement deficit," or a difference between regulatory intentions and the ability to practically enforce.

3.1.1 Independence and Accountability Concerns

The DPB's composition and appointment process raise significant concerns about regulatory independence. All Board members, including the Chairperson, are appointed by the Central Government with terms and service conditions prescribed by central rules. This structure lacks the statutory guarantees of independence that characterize effective regulatory bodies.

Legal analysis reveals that Section 27(3) of the DPDP Act enables the Central Government to issue directions that the DPB "may modify or suspend" its own orders based on government reference. This provision effectively grants the executive branch veto power over the Board's decisions, particularly problematic when government entities are involved in data protection violations.

3.1.2 Capacity and Resource Constraints

There may not be a capacity for effective oversight of a national board that oversees all data processing that occurs across diverse sectors and geographies. Research suggests that centralized authorities in other

eISSN 3049-2610
Research Stream
A Bi-Annual, Open Access Pear Reviewed International Journal
Volume 03, Issue 01, March 2026

jurisdictions are less concerned with smaller violations and instead focus on prominent cases. Consequently, many data handlers may be implicitly under-regulated.

The absence of regional offices or state-level enforcement mechanisms limits the Board's ability to conduct effective investigations and provide accessible grievance redressal for citizens. This geographic disconnect is particularly problematic in India's federal structure, where states manage significant personal data systems for healthcare, education, and public distribution programs.

3.2 Disproportionate Compliance Burdens on MSMEs

India has over 63 million Micro, Small and Medium Enterprises (MSMEs) that comprise the backbone of the economy. The DPDP Act includes uniform compliance obligations, regardless of size, which places disproportionate burdens on these entities that do not have the resources or technical expertise of larger companies.

Survey research by the India SME Forum reveals that only 2.5% of surveyed MSMEs understand the DPDP Act's requirements, indicating a significant awareness gap. Unlike large corporations with dedicated compliance departments, MSMEs operate with limited human and financial resources, making compliance implementation particularly challenging.

The Act requires MSMEs to implement comprehensive data protection measures including consent management systems, breach notification protocols, data protection impact assessments, and grievance redressal mechanisms. For a small tailoring shop or local bakery, these requirements necessitate new hardware, internet connectivity, software subscriptions, cybersecurity measures, and staff training - costs that many cannot afford.

3.2.2 Technical Infrastructure Challenges

The DPDP Act's assumption that all entities operate with robust digital infrastructure misreads India's MSME landscape. Many MSMEs rely on basic technology systems that lack privacy-by-design capabilities. Upgrading these systems to meet the Act's requirements for encryption, data minimization, audit logs, and consent tracking represents a significant technical and financial challenge.

Research indicates that for MSMEs, customer data is often incidental rather than strategic, with trust built through service quality and personal relationships rather than complex consent flows. The Act's techno-legal framework, designed for digitally mature entities, may not align with the operational realities of traditional small businesses.

3.3 Consent Management Complexities and User Experience Challenges

The DPDP Act puts emphasis on consent being central to its data protection obligations, and outlines that consent must be "free, specific, informed, unconditional, and unambiguous". However, ensuring users' consent management systems are ambiguous and that businesses uphold these obligations present challenges.

3.3.1 Granular Consent Requirements

The recently released Business Requirement Document (BRD) for consent management mandates highly granular, purpose-specific consent without clear guidance on grouping related purposes. This requirement

creates operational complexities, particularly for multi-service platforms that process data for various interconnected purposes.

Industry analysis has launched the term "consent fatigue," which means that consent requests can be repeated so frequently they become meaningless and irrelevant. This is harmful to both the interest of having effective consent, but also to the overall user experience.

3.3.2 Technical Implementation Challenges

The BRD's consent management architecture requires real-time consent validation, multilingual consent notices, consent artifact generation with complete metadata tracking, and seven-year digital record retention. These technical requirements assume API-ready systems and sophisticated data management capabilities that many organizations, particularly smaller ones, may not possess.

Research indicates that the consent management framework's complexity may not be sustainable across India's diverse digital ecosystem, particularly in sectors with low-tech operations or offline customer interactions. The requirement for Consent Managers with minimum net worth of ₹2 crore further concentrates this critical function among a limited number of entities.

3.4 Cross-Border Data Transfer Regulatory Uncertainty

The DPDP Act takes a "blacklist" approach to cross-border data transfers, which allows personal data to be transferred to any country, except for those formally blacklisted by the Central Government. However, with this approach, businesses operating across multiple jurisdictions are stuck in an exceedingly uncertain regulatory environment.

3.4.1 Lack of Transparent Criteria

The DPDP Act does not have an adequacy assessment framework like the GDPR's, and it does not promulgate clear standards for which countries might be blacklisted. This confusing regulatory uncertainty in the absence of standards will strain businesses making decisions about what regulatory restrictions they face in transferring data across borders.

Legal analysis indicates that the Central Government's ability to blacklist at will (without justifying its decisions or consulting with industry sources), represents a broad exercise of discretion that creates a uncertain regulatory environment. Businesses must continuously monitor government notifications while lacking any mechanism to challenge or appeal blacklisting decisions.

3.4.2 Impact on Global Operations

The regulatory uncertainty surrounding cross-border transfers particularly affects India's significant IT services sector and multinational corporations. Companies relying on global cloud infrastructure or international data processing arrangements face potential compliance risks if their service providers are located in jurisdictions that may be blacklisted.

Research shows the uncertainty with cross-border compliance could also impact India's role as a global IT platform, affecting its competitiveness in technology services and digital innovation. The lack of alternative transfer mechanisms (such as Standard Contractual Clauses or Binding Corporate Rules) only serves to further complicate the regulatory compliance needs of businesses working internationally.

eISSN 3049-2610
Research Stream
A Bi-Annual, Open Access Pear Reviewed International Journal
Volume 03, Issue 01, March 2026

3.5 Conflicts with Existing Legal Frameworks

The DPDP Act's implementation creates potential conflicts with existing legislation, particularly the Right to Information (RTI) Act, 2005, and sectoral regulations governing financial services.

3.5.1 RTI Act Tensions

The DPDP Act introduces amendments to Section 8(1)(j) of the RTI Act which would allow for an exemption to disclosure of personal information of public officials, even where the public interest weighs in favor of disclosure. This tension between transparency and privacy will ultimately have an implication on the efficacy of the RTI Act to hold governments accountable.

Some scholars note that this conflict is a result of inadequate harmonization of privacy protections with existing transparency schemes, and may ultimately lead to legal uncertainty for public authorities receiving and accounting for information requests.

3.5.2 Sectoral Regulatory Conflicts

The DPDP Act's interaction with sectoral regulations, particularly in financial services, creates additional compliance complexities. The Reserve Bank of India's data localisation requirements for processing payment data may create conflicts with the DPDP Act's provisions for cross-border transfers which would create uncertainty for financial institutions.

This ambiguity may also be exacerbated by the oft-discussed lack of mechanisms for inter-regulatory coordination, resulting in duplicated or conflicting obligations, and the overall financial burden and legal risk that may stem from working with multiple regulations that business are subjected to.

IV. Analysis and Discussion

4.1 Structural Design Flaws

The implementation challenges facing the DPDP Act largely stem from structural design choices that prioritize legislative simplicity over implementation feasibility. The centralized enforcement model, while administratively efficient, fails to account for India's federal governance structure and the diverse needs of different sectors and regions.

The Act's heavy reliance on consent as the primary legal basis for processing, while conceptually empowering for individuals, creates practical difficulties in implementation that may ultimately undermine user privacy rather than protect it. The absence of alternative lawful bases for processing, such as legitimate interests or contractual necessity, forces all data processing activities through the consent bottleneck.

4.2 Proportionality and Fairness Concerns

Using identical compliance obligations across firms of differing sizes and capacities raises legitimate concerns around proportionately and fairness of regulation. The Act's failure to introduce a tiered set of obligations based on size, risk profile, or sectoral characteristics could inhibit innovation and entrepreneurship across India's digital economy.

Comparative analysis with successful data protection regimes reveals the importance of calibrated compliance mechanisms that recognize the different capabilities and risk profiles of various entities. The GDPR's

provisions for small and medium enterprises, including simplified obligations and regulatory guidance, offer models that could inform DPDP Act implementation.

4.3 Regulatory Capacity and Governance

The issues around implementation also speak of wider challenges with regulatory ability and governance within India's policy landscape around digital. The hurriedness of the legislative process with little parliamentary debate or consultation from stakeholders has resulted in a law that lacks much of the implementation guidance required for its compliance.

Stakeholders have therefore had to attempt to interpret and implement the requirements of the Act without any precursor institutions, regulatory sandboxes, or pilot programs to support or guide them. This regulatory vacuum leaves smaller firms, in particular, at a disadvantage due to their inability to engage more expert legal and technical resources to assist with compliance or interpretation.

V. Recommendations and Way Forward

5.1 Decentralized Enforcement Architecture

To tackle the enforcement gap, India may consider establishing state-level Data Protection Boards or regional levels of the central Board. This federated approach would provide greater geographic coverage, local perspective, and access to grievance mechanisms for citizens.

The manner in which the DPB is constituted and governed should be amended to provide greater independence from the executive branch, possibly through judicial appointment processes and/or multi-stakeholder appointment mechanisms.

5.3 Consent Management Simplification

The consent management framework should be streamlined for user ease while keeping meaningful choice intact. This could include templates for standard consent forms, a consolidated consent process for related purposes, and industry specific guidance on choices related to any related purposes.

The concept of specialized Consent Managers should also be considered for removal or simplification, allowing small organizations to use a simple consent management solution without significant investment in infrastructure.

5.4 Regulatory Clarity and Guidance

The government must provide comprehensive implementation guidance, from sector-specific guidance, to standard operating procedure and practical tools that facilitate compliance. Further establishing straightforward criteria for making decisions about cross-border transfers and transparency about the regulatory process would reduce uncertainty in the business environment. Ongoing stakeholder consultations and feedback processes should be necessary to ensure issues around implementation are identified and addressed in a timely and effective manner.

VI. Conclusion

The DPDP Act, 2023 marks a huge step forward in India's data protection ecosystem, establishing important rights around privacy and offerings of regulatory frameworks. However, moving from legislative intent to

practice has revealed major obstacles to the Act's intended outcomes and aimed outcomes for a digital economy.

The centralised enforcement architecture generates an enforcement deficit that could leave violation unaddressed while reinforcing the regulatory power structure both format the layers of reporting mechanisms, not to mention inducing a regulatory enforcement paradigm of thinning the line of independence and accountability. The uniform compliance framework applies disproportionate burden on MSME's potentially stifling innovation and economic grow in sectors which are vital in building India's economy.

An ongoing convoluted consent management process, uncertainty in transfer regulations, and conflicts with the current legal framework, introduces even more challenges to implementation. These challenges represent deeper, structural issues in the design, which sacrifices implementation viability with regulatory simplicity.

Overcoming these implementation difficulties requires a multifaceted response, including a decentralized enforcement mechanism, tiered compliance requirements, simplified consent management framework, as well as comprehensive regulatory guidance. Finally, the efficacy of India's data protection regime, if and when it comes to fruition, will largely rely not on the sophistication of legal provisions but on the practical capacity of implementation mechanisms and responses to the data protection law.

DPDP Act implementation challenges provide valuable insights for uttering governance in developing economies, and also suggest a need for regulatory frameworks to balance privacy protection and economic development objectives, while accounting for diverse stakeholder capabilities and needs. As India seeks to hone its data protection framework over the next several years, addressing implementation challenges will be essential to meet the framework's stated objectives, as indicated in the DPDP Act -meet the stated objectives, protect individual privacy while enabling digital innovation and economic development.

Going forward, collaboration between regulators, industry, and civil society will be necessary to devise solutions that render data protection feasible and attainable across a diverse Indian digital ecosystem. It is only by combining knowledge, capacity, and resourcefulness in the face of the implementation challenges, that the DPDP Act can fulfil its purpose of making India a global leader in privacy-protective digital governance.

References

1. Anuj Agarwal, India's Digital Personal Data Protection Act, 2023: A Landmark Step Forward, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (Oct. 2, 2023), https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law.asiapacific
2. Vaibhav Dharod & Kevin Tauro, Assessing India's Digital Personal Data Protection Act, 2023: A Comparative Study with the GDPR, INT'L J. OF LEGAL & LEGISLATIVE REVIEWS (Apr. 12, 2025).
3. Techno-Legal DPDP Framework Misreads India's MSME Landscape, INCLUSION.IN (Apr. 28, 2025), https://inclusion.in/news/2025/04/techno-legal-dpdp-framework-misreads-indias-msme-landscape/.indianrajniti
4. Data Protection Board of India: A Watchdog Without Teeth, SOFTWARE FREEDOM LAW CENTRE (Feb. 5, 2025), https://sflc.in/data-protection-board-of-india-a-watchdog-without-teeth/.policyreview

5. The Recent "Business Requirement Document" on Consent, CYRIL AMARCHAND MANGALDAS (June 18, 2025), https://corporate.cyrilamarchandblogs.com/2025/06/the-ghost-in-the-machine-the-recent-business-requirement-document-on-consent/.
6. Understanding India's New Data Protection Law, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (Oct. 2, 2023), https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law.
7. Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023, HIGHER SCHOOL OF ECONOMICS (July 1, 2025), https://lida.hse.ru/article/view/27529.
8. Enforcement Gaps in India's DPDP Act and the Case for Decentralized Data Protection Boards, EXPRESS COMPUTER (July 3, 2025), https://www.expresscomputer.in/guest-blogs/enforcement-gaps-in-indias-dpdp-act-and-the-case-for-decentralized-data-protection-boards/126140/.
9. Data Protection Board | Digital Personal Data Protection Act, FOX MANDAL (Sept. 25, 2023), https://foxmandal.in/data-protection-board-implications-of-absence-of-judicial-member/.
10. Centre for Internet & Soc'y & Info. Pol'y Ctr., The Limitations of Consent as a Legal Basis for Data Processing, BURKHARDT KLAUS LEGAL (Dec. 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_bkl_limitations_of_consent_legal_basis_data_processing_dec24.pdf
11. Filipe Brito Bastos, Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?, 19 EUR. CONST. L. REV. 454 (2023), available at https://journals.sagepub.com/doi/abs/10.1177/20414086231203056
12. Juliana Abrusio, The (In)Efficacy of Consent for Processing of Personal Data, 6 HUM. & RTS. 181 (2024), available at https://www.cambridge.org/engage/api-gateway/duke/content/item/641aacf5f6d6a3712d8a9548/fulltext.pdf
13. Charu Malhotra & Roli Nigam, Digital Personal Data Protection (DPDP) Act 2023 of India: A Critical Analysis, 72 INDIAN J. PUB. ADMIN. 1 (2024), available at https://journals.sagepub.com/doi/abs/10.1177/025376482410069
14. Graham Greenleaf, India's 2023 Data Privacy Act: Business/Government Surveillance Without 'Irritants', 189 PRIVACY L. & BUS. INT'L REP. 1 (2023), available at https://journals.sagepub.com/doi/10.1177/02537176251370651
15. Anirudh Burman & Suyash Rai, Understanding India's New Data Protection Law, CARNEGIE ENDOWMENT FOR INT'L PEACE (Oct. 2, 2023), available at https://carnegieendowment.org/research/2023/10/02/understanding-indias-new-data-protection-law
16. India's Cross-Border Data Transfer Regulation, INFO. TECH. & INNOVATION FOUND. (June 9, 2025), available at https://itif.org/publications/2025/06/09/india-cross-border-data-transfer-regulation/
17. Pakhi Garg & Keta Mittal, India's Transparency Quandary: RTI versus DPDP, SCC ONLINE BLOG (Aug. 11, 2025), available at https://www.scconline.com/blog/post/2025/08/11/indias-transparency-quandary-rti-versus-dpdp/
18. Challenge of Balancing Privacy and Transparency, INDIA F. (June 6, 2025), available at https://www.theindiaforum.in/public-policy/challenge-balancing-privacy-and-transparencypapers.ssrn
19. Akanksha Nagar, Consent Fatigue, MSME Strain, and AI Hurdles: Contentious Corners of DPDP Act, STORYBOARD18 (Sept. 21, 2025), available at https://www.storyboard18.com/digital/consent-fatigue-msme-strain-and-ai-hurdles-contentious-corners-of-dpdp-act-81247.htm