IJVAST | Vol. 2, Issue 3 | July 2026 | Open Access — Peer Reviewed Research Paper

Data Privacy under DPDP Act 2023: Challenges and Compliance

Khushi. Chatterjee[1], Rohan. Mehta[2]
Department of Law and Legal Studies
National Law School of India University, Bangalore, Karnataka, India

Abstract—India's Digital Personal Data Protection (DPDP) Act 2023 marks a watershed moment in the country's legal landscape, establishing for the first time a comprehensive statutory framework governing the collection, processing, storage, and transfer of personal data. Enacted on 11 August 2023 and applicable to the world's most populous digital economy with over 900 million internet users, the Act imposes significant compliance obligations on data fiduciaries across sectors. This review paper critically examines the key provisions of the DPDP Act 2023 — including consent architecture, data principal rights, obligations of significant data fiduciaries, cross-border transfer restrictions, children's data protections, and the penalty framework. A systematic comparative analysis with the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA) is presented. Case studies of compliance challenges in the fintech, edtech, and healthcare sectors are analysed. A structured compliance checklist of 10 actionable items for small and medium enterprises (SMEs) is developed. The paper identifies four critical compliance gaps: consent management infrastructure, cross-border transfer uncertainty, data localisation for cloud platforms, and children's data verification. Future directions include monitoring delegated legislation, building privacy-by-design architectures, and cross-sector compliance benchmarking.

Index Terms—DPDP Act 2023, Data Privacy, India, GDPR, CCPA, Consent Management, Data Fiduciary, Cross-border Transfer, Significant Data Fiduciary, SME Compliance, Digital Personal Data, Data Principal Rights, Penalty Framework, Privacy Law.

I. INTRODUCTION

The enactment of the Digital Personal Data Protection (DPDP) Act 2023 represents India's most significant legislative step in data governance since the Information Technology Act 2000. India's digital economy, valued at over $1 trillion and growing at 15% annually, generates enormous volumes of personal data across e-commerce, fintech, healthcare, education, and social media platforms. Prior to the DPDP Act, data protection in India was governed by fragmented provisions under Section 43A of the IT Act 2000 and the IT (Reasonable Security Practices) Rules 2011 — an inadequate framework for the scale and complexity of modern data processing.

The DPDP Act 2023 was preceded by over five years of legislative deliberation. The Justice B.N. Srikrishna Committee submitted its foundational report 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' in 2018 [1]. Two subsequent Personal Data Protection Bills (2019, 2021) were introduced in Parliament before being withdrawn, culminating in the leaner, principles-based DPDP Act 2023 assented to by the President on 11 August 2023 [2].

The Act's passage follows a global trend toward comprehensive data protection legislation initiated by the

D. Significant Data Fiduciaries — Section 10

The Government may designate certain data fiduciaries as 'Significant Data Fiduciaries' (SDFs) based on the volume and sensitivity of personal data processed, risk to data principals, potential impact on national security, sovereignty, or public order, or risk to electoral democracy [Section 10(1)]. SDFs face additional obligations: appointment of a Data Protection Officer (DPO) resident in India, engagement of an independent Data Auditor, and conduct of Data Protection Impact Assessments (DPIAs). Large technology platforms, social media companies, fintech platforms, and health data processors are expected to be designated as SDFs once the criteria are notified through subordinate rules.

E. Children's Data — Section 9

Section 9 prohibits the processing of personal data of minors (under 18 years) without verifiable parental consent. Additionally, data fiduciaries are prohibited from processing children's data in a manner that is likely to cause detrimental effects on the child's well-being or involves tracking, behavioural monitoring, or targeted advertising. This provision has profound implications for edtech platforms, gaming apps, social media companies, and streaming services operating in India — all of which must implement robust age

GDPR in 2018, which has since influenced over 130 countries to enact or update privacy laws [3]. Unlike the GDPR, the DPDP Act adopts a more streamlined, business-friendly approach, avoiding overly prescriptive procedural requirements while establishing clear rights for data principals and obligations for data fiduciaries.

This paper makes the following contributions: (1) a comprehensive analysis of the DPDP Act 2023's key provisions and their operational implications; (2) a systematic comparative analysis with GDPR and CCPA; (3) sector-specific compliance case studies for fintech, edtech, and healthcare; (4) a structured SME compliance checklist; and (5) identification of critical compliance gaps and future research directions.

II. BACKGROUND AND LEGAL CONTEXT

A. Pre-DPDP Legal Landscape in India

Before the DPDP Act, personal data protection in India relied on Section 43A of the IT Act 2000, which imposed liability on companies holding sensitive personal data if they failed to implement reasonable security practices [4]. The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 defined sensitive personal information (SPI) and required consent for its collection. However, these rules applied only to companies and did not cover government data processing, lacked a dedicated regulatory authority, and imposed minimal penalties — wholly insufficient for modern data ecosystems.

B. Global Data Protection Landscape

The European Union's GDPR [5], effective May 2018, established the global benchmark for data protection, introducing the principles of data minimisation, purpose limitation, storage limitation, accuracy, integrity, and confidentiality as binding legal obligations. GDPR established the rights to access, rectification, erasure (right to be forgotten), restriction of processing, portability, and object to automated decision-making. Fines of up to EUR 20 million or 4% of global annual turnover, whichever is higher, have been imposed on major corporations including Meta (EUR 1.2 billion), Amazon (EUR 746 million), and WhatsApp (EUR 225 million).

California's CCPA [6], effective January 2020 and strengthened by the CPRA in 2023, grants Californian consumers the right to know what personal information is collected, the right to delete, the right to opt-out of data sales, and the right to non-discrimination. Unlike GDPR, CCPA does not require consent for data processing but provides opt-out rights and applies only to for-profit businesses meeting verification and parental consent mechanisms [9].

F. Cross-Border Data Transfers — Section 16

Section 16 permits transfer of personal data to countries or territories outside India that the Central Government may notify — a 'whitelist' approach that contrasts with GDPR's adequacy decision and Standard Contractual Clauses (SCCs) framework. The list of notified countries had not been published as of 2025, creating significant uncertainty for multinational companies, cloud service providers, and SaaS platforms operating in India and transferring data to servers located overseas. Pending notification, organisations must assess cross-border transfer risks and prepare compliant data transfer mechanisms [10].

G. Penalty Framework — Section 33–40

The DPDP Act 2023 establishes a tiered penalty structure enforced by the Data Protection Board of India. Penalties range from Rs. 50 crore for failure to notify data breaches (Section 8(6)) to Rs. 250 crore for failure to protect children's data (Section 9). The maximum aggregate penalty under the Act is Rs. 500 crore. Compared to the IT Act 2000's maximum penalty of Rs. 5 crore under Section 43A, these penalties represent a 100x increase in maximum liability — fundamentally altering the risk calculus for non-compliant organisations.

IV. COMPARATIVE ANALYSIS WITH GDPR AND CCPA

The comparative analysis presented in Table I reveals significant structural similarities between the DPDP Act 2023 and GDPR in consent requirements, data principal rights, and breach notification obligations. However, three critical differences distinguish the Indian framework: the absence of mandatory data portability rights; broader deemed consent provisions for State data processing; and the whitelist cross-border transfer approach rather than the GDPR's more flexible adequacy mechanism.

Compared to CCPA, the DPDP Act imposes more comprehensive obligations — applying to all data fiduciaries regardless of revenue threshold — while adopting an opt-in consent model rather than CCPA's opt-out approach. The DPDP Act's children's data provisions are more stringent than both GDPR (which sets the age limit at 16, with Member State flexibility down to 13) and CCPA's reliance on COPPA for children's data [11].

V. SECTOR-SPECIFIC COMPLIANCE CASE STUDIES

A. Fintech Sector

specific revenue or data processing thresholds.

C. The Srikrishna Committee and Legislative Journey

The Justice Srikrishna Committee's 2018 report proposed a comprehensive data protection regime with a powerful Data Protection Authority (DPA), mandatory data localisation for critical personal data, and wide-ranging data principal rights [1]. The PDP Bill 2019 largely adopted these recommendations but faced criticism for excessive government exemptions. The PDP Bill 2021 introduced significant amendments before both bills were withdrawn in 2022. The DPDP Act 2023 emerged as a more concise legislation, with many implementation details delegated to subordinate rules — the DPDP Rules, which remained in draft form as of 2025 [7].

III. KEY PROVISIONS OF THE DPDP ACT 2023

A. Consent Architecture — Section 6 and 7

The Act requires consent to be free, specific, informed, unconditional, and unambiguous, expressed through a clear affirmative action [Section 6]. Consent must be accompanied by a notice informing the data principal of the personal data to be collected, the purpose of processing, and the manner in which rights may be exercised. Critically, consent is withdrawable at any time, with the ease of withdrawal required to be comparable to the ease of giving consent — placing a direct obligation on organisations to build consent revocation mechanisms into their customer-facing platforms.

Section 7 provides that certain processing does not require consent — including performance of a function of the State, compliance with a law or court order, employment purposes, and medical emergencies — a broader set of lawful bases than those originally proposed in draft bills. These deemed consent provisions have attracted significant criticism for their potential to allow extensive State data processing without meaningful oversight [8].

B. Data Principal Rights — Sections 11–14

The Act codifies four rights for data principals: the right to access information about personal data processed (Section 11); the right to correction, completion, updating, and erasure of personal data (Section 12); the right to grievance redressal within a prescribed timeline (Section 13); and the right to nominate another person to exercise rights in the event of death or incapacity (Section 14). Notably absent from the DPDP Act, compared to GDPR, are explicit rights to data portability and the right to object to automated decision-making — significant gaps from a digital rights perspective.

C. Obligations of Data Fiduciaries — Section 8

Data Fiduciaries — any person or entity that processes

Digital payment and lending platforms process extremely large volumes of sensitive personal data including financial transaction history, bank account details, PAN/Aadhaar numbers, credit bureau data, and geolocation. Under the DPDP Act, these platforms must obtain specific consent for each processing purpose — a significant departure from the current common practice of a single omnibus privacy policy. Critical compliance actions for fintech include: (1) disaggregating consent across processing purposes in their apps; (2) building real-time data erasure APIs for customer accounts; (3) establishing cross-border transfer controls for international payment networks; and (4) conducting DPIAs if designated as Significant Data Fiduciaries [12].

B. EdTech Sector

India's edtech sector, valued at $6 billion and serving over 50 million students, processes substantial children's data. Section 9's verifiable parental consent requirement is particularly burdensome for edtech platforms that must now implement age verification at registration and obtain verifiable parental consent — technically challenging for low-smartphone-penetration geographies. Additionally, the prohibition on behavioural profiling of minors directly conflicts with the personalised learning recommendation engines that constitute the core technology differentiator for most edtech platforms [13].

C. Healthcare Sector

Healthcare data represents the most sensitive category of personal information. While the DPDP Act does not separately categorise 'sensitive personal data' as the predecessor PDP Bills did, health data processing by hospitals, telemedicine platforms, health insurance companies, and medical device manufacturers will be subject to the full consent and fiduciary obligations of the Act. The deemed consent provision for medical emergencies provides limited relief. Healthcare organisations must implement consent management systems capable of distinguishing between treatment-related processing (deemed consent) and research or commercial processing (explicit consent required) [14].

VI. CRITICAL COMPLIANCE GAPS

A. Consent Management Infrastructure

The Act's requirement for purpose-specific, withdrawable consent with equal ease of withdrawal creates an immediate need for Consent Management Platforms (CMPs) integrated with organisational CRM, marketing automation, and data warehousing systems. Most Indian enterprises, particularly SMEs, currently lack the technical infrastructure to implement granular consent management at the scale required

personal data — are subject to comprehensive obligations under Section 8. These include: processing personal data only for the purpose for which consent was obtained (purpose limitation); ensuring completeness, accuracy, and consistency of personal data used for decisions affecting data principals; implementing appropriate technical and organisational measures to ensure compliance with Act provisions; and notifying the Data Protection Board and affected data principals in the event of a personal data breach without delay [Section 8(6)].

by the Act — representing both a compliance gap and a significant technology market opportunity [15].

B. Cross-Border Transfer Uncertainty

The failure to notify the list of approved countries for cross-border data transfer under Section 16 creates substantial operational uncertainty for cloud-hosted SaaS platforms, international payment networks, and global technology companies operating in India. Until the whitelist is published, organisations face an unresolved compliance risk for all cross-border transfers — potentially requiring emergency data architecture changes upon notification [10].

C. Children's Data Verification

Implementing technically reliable, scalable, and affordable age verification and verifiable parental consent mechanisms for minors under Section 9 remains unsolved at the industry level. There is no government-provided age verification infrastructure, and third-party solutions raise additional privacy concerns by requiring even more personal data. The Rules are expected to provide implementation guidance, but until then companies face an implementation vacuum [9].

D. SME Awareness and Capacity Gap

India's 6.3 crore SMEs are largely unaware of DPDP Act obligations and lack the legal, technical, and financial resources to implement compliance programmes. The Act applies to all data fiduciaries regardless of size — unlike GDPR's SME exemptions for organisations with fewer than 250 employees. Targeted government guidance, industry association awareness programmes, and affordable compliance technology solutions will be critical to achieving meaningful SME compliance [16].

TABLE I — Comparative Analysis: DPDP Act 2023 vs. GDPR vs. CCPA

Provision	DPDP Act 2023	GDPR (EU)	CCPA (California)	Impact on India
Consent Model	Explicit, specific, withdrawable	Freely given, specific, informed	Opt-out for data sale	Major CRM overhaul required
Right to Erasure	Yes — Section 13	Yes — Article 17	Yes — CCPA	Data lifecycle redesign
Cross-border Transfer	Notified countries only	Adequacy decision / SCCs	No restriction	SaaS cloud uncertainty
Max Penalty	Rs. 250 Crore	EUR 20 Million / 4% turnover	USD 7,500 per violation	Higher than IT Act 2000
Children's Data	Under 18 — verifiable consent	Under 16 — parental consent	Under 16 — COPPA	EdTech/apps critical impact
DPO Requirement	Significant Data Fiduciary only	Mandatory in many cases	Not required	Large enterprises affected
Breach Notification	Data Protection Board	72 hours to supervisory auth.	Law enforcement only	New compliance pipeline needed

TABLE II — DPDP Act 2023 SME Compliance Checklist — 10 Critical Action Items

#	Compliance Action Item	Applicable To	Priority	DPDP Section
1	Audit all personal data collection points	All Data Fiduciaries	Critical	Section 4, 5

2	Implement consent management platform	All businesses	Critical	Section 6, 7
3	Enable right of access mechanism	All Data Fiduciaries	High	Section 11
4	Build data erasure / correction API	Apps, platforms, banks	High	Section 12, 13
5	Verify cross-border transfer destinations	SaaS, cloud companies	Critical	Section 16
6	Appoint Data Protection Officer (DPO)	Significant Data Fiduciaries	High	Section 10
7	Add verifiable parental consent for minors	EdTech, gaming, social media	Critical	Section 9
8	Establish data breach notification process	All Data Fiduciaries	High	Section 8(6)
9	Update vendor/processor agreements	All businesses	Medium	Section 8
10	Conduct Data Protection Impact Assessment	Significant Data Fiduciaries	Medium	Section 10(2)

VII. FUTURE RESEARCH DIRECTIONS

A. Monitoring DPDP Rules and Notified Countries

The DPDP Act 2023 is an enabling statute — its operational impact will be determined by subordinate legislation including the DPDP Rules and the no tified whitelist of countries approved for cross-bo rder data transfer. Future research should systematically track rule-making, analyse their compliance implications, and compare India's evolving framework with amendments to GDPR and emerging data protection regimes in Southeast Asia and the Gulf Cooperation Council [17].

B. Privacy-by-Design Implementation

The DPDP Act's emphasis on purpose limitation and data minimisation aligns with the privacy-by-design principle advocated by regulators globally. Research into privacy-by-design engineering frameworks specifically adapted to Indian software development practices, technology stacks, and business process contexts will be critical for enabling organisations to build compliance into product architecture rather than retrofitting it [18].

C. AI and Automated Decision-Making

The DPDP Act 2023 does not explicitly address artificial intelligence or automated decision-making — a significant gap given India's rapidly growing AI adoption in credit scoring, insurance underwriting, recruitment, and public benefits administration. As India develops its National Data Governance Framework and AI regulatory policy, research into the interaction between the DPDP Act's consent requirements and AI-driven personal data processing will be of increasing importance [19].

D. Empirical Compliance Benchmarking

Empirical studies assessing the actual state of DPDP Act compliance across Indian industries — using structured surveys, privacy policy audits, app permission analysis, and Technical compliance testing — will provide evidence-based insights for regulators, industry associations, and technology solution providers. Longitudinal benchmarking tracking compliance maturity over multiple years following Act implementation would constitute a valuable contribution to the data governance literature [16].

VIII. CONCLUSION

The Digital Personal Data Protection Act 2023 represents a pivotal milestone in India's data governance journey — establishing for the first time a comprehensive, rights-based framework for the protection of personal data across the world's largest digital democracy. This review has systematically analysed the Act's key provisions, compared them with GDPR and CCPA, examined sector-specific compliance challenges in fintech, edtech, and healthcare, and developed a 10-item compliance checklist for SME data fiduciaries.

The evidence demonstrates that the DPDP Act imposes significant and immediate compliance obligations — particularly in consent management, children's data protection, cross-border transfer governance, and breach notification — requiring fundamental changes to data processing architectures, vendor agreements, and customer-facing interfaces across Indian industry.

Four critical compliance gaps have been identified: the absence of ready consent management infrastructure at scale; unresolved cross-border transfer uncertainty pending country whitelist notification; unsolved children's age verification mechanisms; and the SME awareness and capacity deficit. Addressing these gaps will require coordinated action from the Data Protection Board, industry associations, technology providers, and legal practitioners.

Future research should monitor the evolution of subordinate

legislation, empirically benchmark compliance maturity, and investigate the interaction of the DPDP Act with artificial intelligence, blockchain, and cloud computing — the technologies that will define India's digital economy in the decade ahead. The DPDP Act 2023 is not the end of India's data protection journey — it is the beginning.

IX. REFERENCES

[1] Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Ministry of Electronics and Information Technology, New Delhi, 2018.

[2] Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Government of India Gazette, 11 August 2023.

[3] UNCTAD, Data Protection and Privacy Legislation Worldwide, United Nations Conference on Trade and Development, 2024.

[4] Information Technology Act, 2000 (No. 21 of 2000) and IT (Amendment) Act 2008, Government of India.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation — GDPR), Official Journal of the European Union, L 119, 4 May 2016.

[6] California Consumer Privacy Act, Cal. Civ. Code Section 1798.100 et seq. (2018), as amended by the California Privacy Rights Act (CPRA), 2020.

[7] Ministry of Electronics and Information Technology, Draft Digital Personal Data Protection Rules 2025, MeitY, New Delhi, January 2025.

[8] Bhatia, G. and Parsheera, S., An Analysis of the Draft Personal Data Protection Bill 2018, National Law University Delhi and NIPFP, 2018.

[9] Internet Freedom Foundation, Analysis of Children's Data Protection under the DPDP Act 2023, IFF Working Paper, 2024.

[10] Prakash, S. and Jaiswal, A., Cross-border Data Flows under India's DPDP Act: Implications for Cloud Computing, Journal of Indian Law and Society, vol. 15, pp. 42–67, 2024.

[11] Chander, A. and Schwartz, P., Privacy and/or Trade, University of Chicago Law Review, vol. 90, no. 1, pp. 1–52, 2023.

[12] Reserve Bank of India, Data Localisation Requirements for Payment System Operators, RBI Circular DPSS.CO.OD No.2785, 2018.

[13] Mehrotra, S., EdTech and Data Privacy in India: Compliance Challenges under the DPDP Act 2023, Indian Journal of Law and Technology, vol. 19, pp. 112–135, 2024.

[14] NITI Aayog, National Health Data Management Policy, Government of India, 2020.

[15] Deloitte India, India DPDP Act Compliance Survey 2024: Enterprise Readiness Assessment, Deloitte Touche Tohmatsu India LLP, 2024.

[16] NASSCOM, DPDP Act 2023: SME Awareness and Compliance Readiness Report, National Association of Software and Service Companies, 2024.

[17] Future of Privacy Forum, Global Privacy Law Developments 2024, FPF Annual Report, Washington DC, 2024.

[18] Cavoukian, A., Privacy by Design: The 7 Foundational Principles, Information and Privacy Commissioner of Ontario, 2009 (updated 2019).

[19] OECD, OECD Principles on Artificial Intelligence, Organisation for Economic Co-operation and Development, 2019.

[20] International Association of Privacy Professionals, India DPDP Act 2023: Practitioner's Guide, IAPP, Portsmouth, NH, 2024.

[21] Krishnamurthy, V., The India Way: Privacy Law and the Digital Economy, Columbia Journal of Transnational Law, vol. 61, pp. 234–289, 2023.

[22] European Data Protection Board, Guidelines on Consent under Regulation 2016/679 (version 1.1), EDPB, 2020.

[23] Singh, R. and Kohli, A., Fintech Data Compliance in Post-DPDP India, Indian Journal of Finance and Banking, vol. 8, pp. 78–99, 2024.

[24] Menon, M., The Data Protection Board of India: Powers, Functions and Enforcement Mechanisms, National Law School Journal, vol. 22, pp. 1–28, 2024.

[25] World Bank, Digital Development and Data Protection in South Asia, World Bank Group Report, Washington DC, 2023.

[26] MeitY, Annual Report 2023–24, Ministry of Electronics and Information Technology, Government of India, 2024.

[27] Purtova, N., The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law, Law, Innovation and Technology, vol. 10, no. 1, pp. 40–81, 2018.

[28] Greenleaf, G., Global Data Privacy Laws 2023: 162 National Laws, Privacy Laws and Business International Report, 2023.

[29] Chatterjee, K. and Mehta, R., Operationalising the DPDP Act 2023: Sector-wise Compliance Roadmap, Indian Journal of Law and Technology, 2025 (forthcoming).

[30] Data Security Council of India, DPDP Act 2023 Industry Impact Assessment, DSCI, New Delhi, 2024

ISSN: Applied For (2026) | DOI: 10.XXXXX/IJVAST.2026.XXXXX | Open Access — CC BY 4.0 License