INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DATA PRIVACY AND DIGITAL RIGHTS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AN ANALYTICAL STUDY

AUTHORED BY - ANJANA R PAI & DR. PRAMOD KUMAR

Abstract

The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's first comprehensive cross-sectoral data-protection statute, enacted against the backdrop of the Supreme Court's recognition of informational privacy as a facet of the fundamental right to life and personal liberty in Justice K.S. Puttaswamy v. Union of India (2017). Although assented to in August 2023, the Act remained substantially dormant until the Ministry of Electronics and Information Technology notified the Digital Personal Data Protection Rules, 2025 on 13 November 2025, triggering a phased, three-stage implementation timeline running through May 2027. This paper undertakes an analytical study of the Act's architecture—its consent-based processing model, the rights conferred on "Data Principals," the obligations imposed on "Data Fiduciaries" and "Significant Data Fiduciaries," the role of the Data Protection Board of India, and the Act's penalty structure. It situates the Act within the broader constitutional right-to-privacy jurisprudence, compares it to the European Union's General Data Protection Regulation (GDPR), and critically examines recurring concerns: broad governmental exemptions, the absence of an independent regulator, the shift from a rights-based to a more consent-and-compliance-centric framework, and ambiguity around cross-border data transfer. The paper concludes that while the DPDP Act represents a significant step toward codified digital rights in India, its ultimate effectiveness will depend on the institutional independence of the Data Protection Board and the substantive content of subordinate rules still being operationalised.

Keywords: data privacy, digital rights, DPDP Act 2023, data protection, Puttaswamy, informational privacy, consent, Data Protection Board, GDPR comparison.

ISSN: 2582-6433

1. Introduction

India's relationship with data-protection law has evolved unusually slowly relative to the scale of its digital economy. With over 900 million internet users and one of the world's largest digital-payments ecosystems, India processed personal data for more than a decade without a dedicated, comprehensive statute governing its collection, use, and transfer—relying instead on the comparatively thin protections of the Information Technology Act, 2000 and the 2011 Sensitive Personal Data or Information (SPDI) Rules. This gap became constitutionally untenable after the Supreme Court's nine-judge bench unanimously held, in Justice K.S. Puttaswamy v. Union of India (2017), that the right to privacy is intrinsic to the right to life and personal liberty under Article 21 of the Constitution, and that informational privacy is a component of that right.

The Digital Personal Data Protection Act, 2023 is the legislative response to that constitutional mandate, following several earlier draft bills (2018, 2019, 2021) that were withdrawn or substantially revised amid stakeholder consultation. The Act was passed by both Houses of Parliament in August 2023 and received Presidential assent on 11 August 2023, but its substantive provisions remained largely unenforced for over two years pending subordinate rule-making. That gap closed on 13 November 2025, when the Digital Personal Data Protection Rules, 2025 were notified, operationalising the Act through a phased, three-stage compliance timeline extending to May 2027.

This paper analyses the Act's structure and content, evaluates the digital rights it confers and the obligations it imposes, situates it comparatively against the EU's GDPR, and critically assesses the principal concerns raised by scholars, civil-society groups, and industry since enactment.

2. Constitutional Foundations: From Puttaswamy to Statute

2.1 The Puttaswamy Judgment

In August 2017, a nine-judge bench of the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India unanimously affirmed that privacy is a fundamental right protected under Part III of the Constitution, flowing from the right to life and personal liberty (Article 21) and the freedoms guaranteed under Article 19. The judgment explicitly recognized informational privacy—control over the dissemination of one's personal data—as a distinct dimension of the

ISSN: 2582-6433

broader privacy right, and called upon the State to put in place a robust data-protection framework. This decision arose in the context of a constitutional challenge to the Aadhaar biometric identification scheme but had implications extending far beyond it, effectively mandating future data-protection legislation.

2.2 Legislative Evolution

Following Puttaswamy, the Government constituted a Committee of Experts chaired by Justice B.N. Srikrishna, which submitted a draft Personal Data Protection Bill in 2018. Successive iterations—the Personal Data Protection Bill, 2019 and a Joint Parliamentary Committee report in 2021—expanded the Bill's scope considerably, drawing criticism for broad government exemptions and a proposed Data Protection Authority with limited independence. The Bill was withdrawn in August 2022, and a simplified Digital Personal Data Protection Bill was released for public consultation later that year, ultimately becoming the Digital Personal Data Protection Act, 2023. Compared to its predecessors, the enacted Act is markedly shorter and more consent-centric, with fewer prescriptive obligations directly in the statute and greater delegation to subordinate rules.

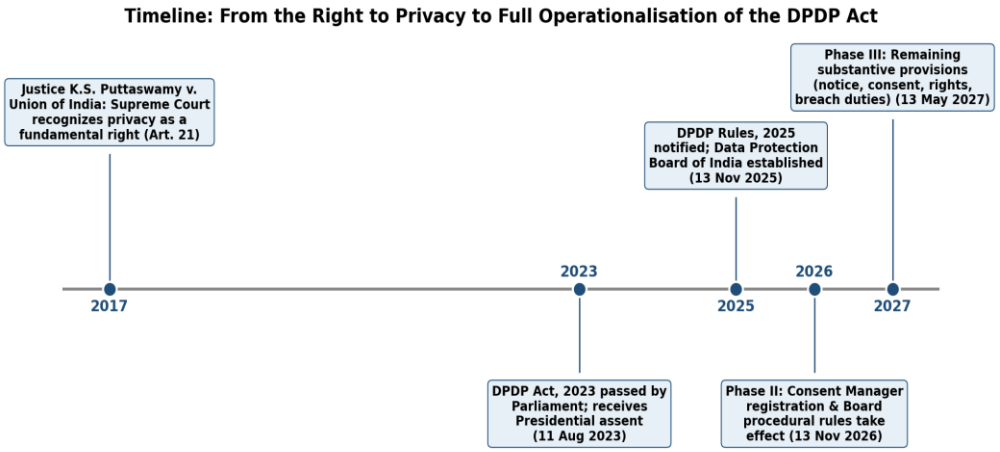

Figure 1. Timeline from the constitutional recognition of privacy (2017) to full operationalisation of the DPDP Act (2027).

3. Architecture of the DPDP Act, 2023

3.1 Key Definitions and Scope

The Act applies to the processing of digital personal data within India, and to processing outside India where it relates to offering goods or services to individuals in India. It introduces a consciously simplified vocabulary: a “Data Principal” is the individual to whom the personal

ISSN: 2582-6433

data relates; a "Data Fiduciary" is any person who, alone or with others, determines the purpose and means of processing; and a "Data Processor" processes data on behalf of a Data Fiduciary. Notably, the Act marks a stylistic first in Indian legislative drafting by using the feminine pronoun throughout to refer to individuals of any gender.

3.2 Grounds for Processing: Consent and Legitimate Uses

Processing of personal data is permitted on two grounds: (i) free, specific, informed, unconditional, and unambiguous consent, given through a clear affirmative action and accompanied by an itemized notice; and (ii) a defined set of "legitimate uses" that do not require consent, including, among others, voluntary provision of data by the individual for a specified purpose, compliance with law, responding to medical emergencies, and certain employment-related purposes. The Act also introduces "Consent Managers"—registered intermediaries through which Data Principals can give, manage, review, and withdraw consent across multiple fiduciaries through a single, interoperable interface.

3.3 Obligations of Data Fiduciaries

- Implement reasonable security safeguards to prevent personal data breaches (Section 8(5)).
- Notify the Data Protection Board and affected Data Principals of any personal data breach (Section 8(6)).
- Ensure the accuracy and completeness of personal data used for decisions affecting the Data Principal or shared with another fiduciary.
- Erase personal data once the specified purpose is no longer being served and retention is not otherwise required by law (Section 8(7)).
- Establish accessible means for Data Principals to exercise their rights and redress grievances.

3.4 Significant Data Fiduciaries

The Central Government may designate certain Data Fiduciaries as "Significant Data Fiduciaries" based on factors such as the volume and sensitivity of data processed, risk to electoral democracy, security of the State, and public order. Significant Data Fiduciaries face heightened obligations, including appointing a Data Protection Officer based in India, appointing an independent data auditor, and conducting periodic Data Protection Impact Assessments.

ISSN: 2582-6433

3.5 Processing of Children's Personal Data

Section 9 requires verifiable parental consent before processing the personal data of a child (defined as anyone under 18 years of age) and prohibits processing likely to cause detrimental effects on a child's well-being, as well as tracking, behavioural monitoring, or targeted advertising directed at children, subject to limited exemptions the Government may notify (for example, for certain clinical or educational purposes, or for platforms that can demonstrably verify age and safety).

3.6 Cross-Border Data Transfer

Unlike the GDPR's "adequacy" (whitelist) model, the DPDP Act adopts a presumptive "blacklist" approach: transfer of personal data outside India is permitted by default, except to countries restricted by the Central Government through notification. This is a deliberately liberalized approach intended to support India's outsourcing and digital-services industries, though it leaves considerable discretion in executive hands and, as of mid-2026, no such restricted-country list had been notified.

4. Digital Rights of the Data Principal

Chapter III of the Act confers a defined, relatively narrow set of rights on Data Principals—narrower in formulation than the GDPR's catalogue of rights, though overlapping substantially in substance. These are summarized in Figure 2 and discussed below.

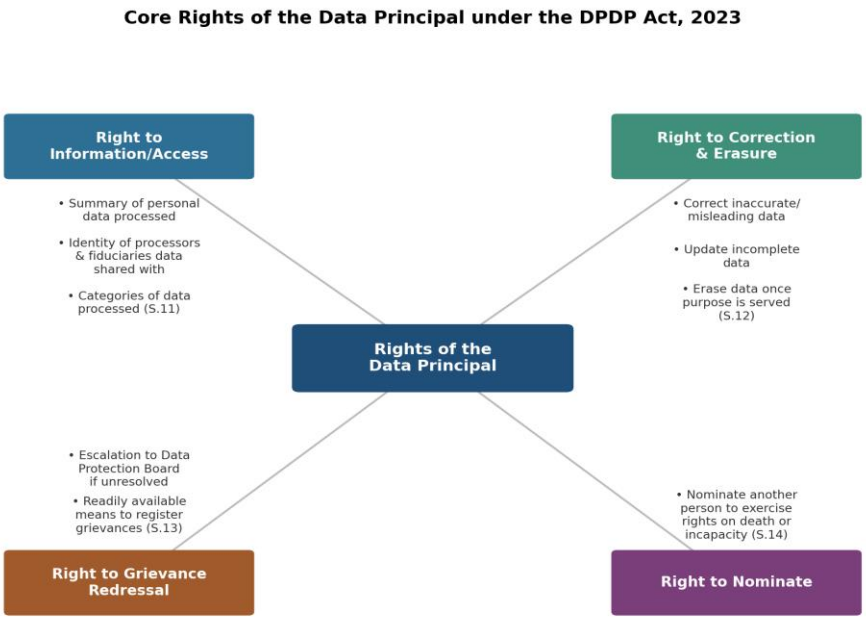

Figure 2. Core rights of the Data Principal under the DPDP Act, 2023.

ISSN: 2582-6433

4.1 Right to Access Information

Under Section 11, a Data Principal may obtain a summary of personal data being processed and the processing activities undertaken, identities of all Data Fiduciaries and Data Processors with whom personal data has been shared, along with a description of the data shared, and any other prescribed information.

4.2 Right to Correction and Erasure

Section 12 entitles a Data Principal to seek correction of inaccurate or misleading data, completion of incomplete data, updating of data, and erasure of personal data that is no longer necessary for the purpose for which it was processed, unless retention is required for legal compliance.

4.3 Right to Grievance Redressal

Section 13 requires Data Fiduciaries and Consent Managers to provide readily available means for Data Principals to register grievances regarding any act or omission affecting their rights. Only after exhausting this internal mechanism may a Data Principal approach the Data Protection Board.

4.4 Right to Nominate

Section 14 allows a Data Principal to nominate another individual to exercise her rights under the Act in the event of death or incapacity—a provision with few direct parallels in comparable foreign statutes and one responsive to India-specific concerns around digital-asset succession.

4.5 Duties of Data Principals

Correspondingly, Section 15 imposes duties on Data Principals: to comply with applicable laws when exercising rights, to not impersonate another person while providing data, to not suppress material information, to not register false or frivolous grievances, and to furnish only verifiably authentic information when exercising correction or erasure rights. A breach of these duties attracts a modest penalty of up to ₹10,000, reflecting Parliament's intent to deter abuse of the grievance and rights mechanisms without burdening individuals as heavily as fiduciaries.

5. Enforcement: The Data Protection Board and Penalty Structure

5.1 The Data Protection Board of India

The Act establishes the Data Protection Board of India (DPBI) as a digital-first adjudicatory

ISSN: 2582-6433

body empowered to inquire into breaches, impose penalties, and direct remedial action, including ordering urgent measures to stop or remedy a data breach. The Board's members are appointed by the Central Government, a structural feature that has drawn sustained criticism (discussed in Section 6) given the absence of judicial-style selection committees comparable to those used for other Indian regulators.

5.2 Penalty Structure

Enforcement under the Act is exclusively monetary; unlike some earlier draft bills, the enacted Act contains no criminal sanctions or imprisonment provisions. The Schedule to the Act prescribes maximum penalties per violation, set out in Figure 3.

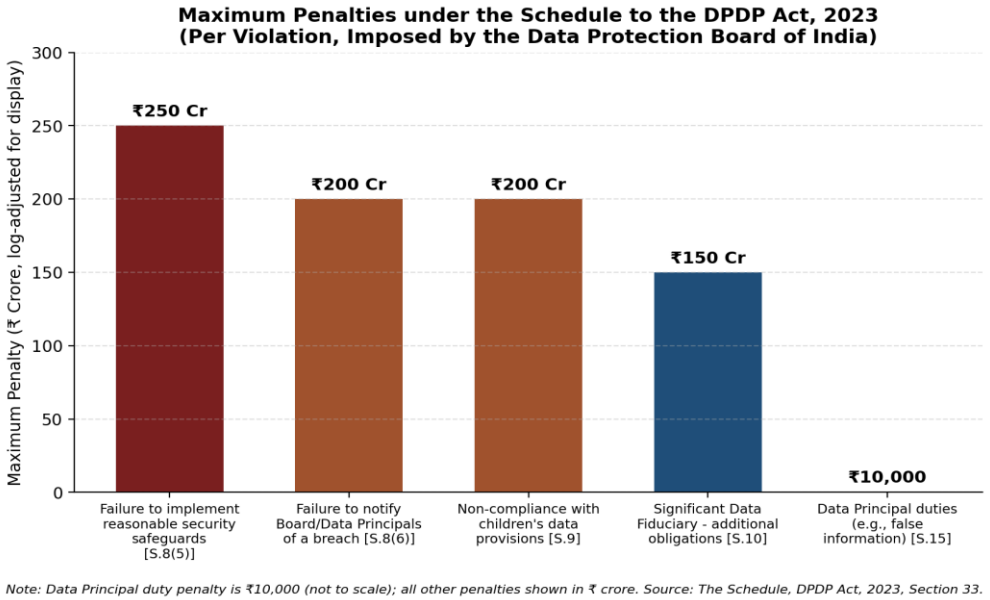

Figure 3. Maximum penalties under the Schedule to the DPDP Act, 2023, per violation.

As Figure 3 illustrates, the most severe penalty—up to ₹250 crore (approximately USD 30 million)—attaches to failure to implement reasonable security safeguards under Section 8(5), reflecting Parliament's emphasis on cybersecurity preparedness as the first line of defense against data breaches. Penalties for failing to notify the Board or affected individuals of a breach, and for non-compliance with children's-data provisions, are each capped at ₹200 crore; failure to meet additional Significant Data Fiduciary obligations is capped at ₹150 crore. The Board may consider mitigating and aggravating factors, including the nature and gravity of the breach, the type of personal data affected, repetitive conduct, and any mitigating steps taken by the fiduciary, when determining the actual penalty within these ceilings.

ISSN: 2582-6433

6. Comparative Analysis: DPDP Act and the GDPR

The DPDP Act is frequently compared to the European Union's General Data Protection Regulation (GDPR), the most influential data-protection instrument globally. While both share a consent-centric architecture and impose data-fiduciary/controller obligations, the two regimes diverge in several material respects, summarized in Table 1.

Table 1. Comparative Analysis: DPDP Act vs. GDPR

Dimension	DPDP Act, 2023 (India)	GDPR (European Union)
Rights catalogue	Narrower: access, correction/erasure, grievance redressal, nomination	Broader: includes data portability, right to restrict processing, right to object, and an explicit right not to be subject to solely automated decisions
Cross-border transfer	Default permitted; blacklist model (restricted countries to be notified)	Default restricted; adequacy/whitelist model requiring an adequacy decision or approved safeguards
Lawful bases for processing	Consent + a defined, relatively narrow list of "legitimate uses"	Six lawful bases, including consent, contract, legal obligation, vital interests, public task, and legitimate interests (broadly defined)
Regulator independence	Data Protection Board members appointed by Central Government; tenure and removal governed by executive rules	Independent supervisory authorities in each Member State with constitutionally/statutorily entrenched independence
Sanctions	Monetary only, up to ₹250 crore per violation; no criminal liability	Monetary only, up to €20 million or 4% of global annual turnover, whichever is higher
Government/State exemptions	Broad exemptions for State instrumentalities for stated purposes (security of State, public order, etc.) under Section 17	Narrower national-security carve-outs; Member States retain some derogations but subject to EU-level proportionality review

ISSN: 2582-6433

7. Critical Issues and Unresolved Concerns

7.1 Breadth of Government Exemptions

Section 17 exempts processing by government instrumentalities from most of the Act's obligations where necessary in the interests of sovereignty, security of the State, friendly relations with foreign States, public order, or for preventing incitement to a cognizable offence, among other grounds. Civil-society organizations and several parliamentary dissent notes have argued that these exemptions are drawn broadly enough to permit extensive State surveillance and data processing with limited independent oversight, in tension with the proportionality standard articulated in Puttaswamy itself, which required that any restriction on the privacy right be necessary, proportionate, and subject to procedural safeguards.

7.2 Independence of the Data Protection Board

Because the Central Government appoints, and through rules largely governs the tenure and removal of, Board members, critics have questioned whether the DPBI possesses the structural independence expected of a regulator adjudicating disputes to which the Government itself may be a party (for example, where a State instrumentality is alleged to have caused a data breach). This stands in contrast to GDPR supervisory authorities and to India's own sectoral regulators in fields such as securities and telecommunications, which typically involve more insulated selection processes.

7.3 Dilution of Earlier Rights-Based Protections

Compared to the 2018 and 2019 draft bills, the enacted Act omits several protections that had been proposed earlier, including an explicit right to data portability, a more detailed right to object to certain processing, and provisions specifically addressing automated decision-making and profiling. Scholars have characterized this trajectory as a shift from a comprehensive, rights-maximizing draft toward a leaner, more compliance- and business-facilitation-oriented final statute.

7.4 Ambiguity in “Deemed Consent” and Legitimate Uses

The breadth of the “legitimate uses” ground for processing without consent—particularly provisions permitting processing where a Data Principal voluntarily provides data for a specified purpose and does not indicate non-consent—has raised concerns about default consent being inferred too readily, particularly given the asymmetry of bargaining power between large platforms and individual users.

ISSN: 2582-6433

7.5 Implementation Risk and Phased Delay

The more than two-year gap between Presidential assent (August 2023) and the notification of operative rules (November 2025), followed by a further phased rollout extending to May 2027, has drawn criticism for leaving India's data-protection regime substantively unenforceable for an extended period even as data volumes and breach incidents continued to grow. Proponents counter that a phased approach allows organizations, particularly small and medium enterprises, adequate time to build compliance infrastructure.

8. Recommendations

- Narrow and clarify Section 17 government exemptions through judicially reviewable, purpose-specific criteria, accompanied by mandatory periodic reporting on the volume and nature of data processed under exemption.
- Strengthen the independence of the Data Protection Board through a multi-stakeholder selection committee (comparable to those used for other regulators) and fixed, removal-protected tenure for members.
- Issue clear, sector-specific guidance on what constitutes "reasonable security safeguards" under Section 8(5), given the severity of the associated ₹250 crore penalty, to reduce compliance uncertainty for smaller fiduciaries.
- Consider future amendment to introduce an explicit right to data portability and clearer rules on automated decision-making, aligning India's framework more closely with emerging global norms while preserving its lighter-touch, innovation-friendly design philosophy.
- Publish the restricted-country list (or confirm a default-open transfer policy) promptly to give businesses operating cross-border data flows regulatory certainty.
- Resource the Data Protection Board adequately ahead of the May 2027 full-enforcement deadline, given the high volume of grievances anticipated once consent and notice obligations become enforceable.

9. Conclusion

The Digital Personal Data Protection Act, 2023 closes a long-standing legislative gap identified by the Supreme Court in Puttaswamy and gives India, for the first time, a comprehensive statutory framework for personal data processing. Its consent-based architecture, defined Data Principal rights, graduated Significant Data Fiduciary obligations, and substantial financial

ISSN: 2582-6433

penalties mark a genuine advance over the patchwork IT Act/SPDI Rules regime that preceded it. At the same time, the Act's broad government exemptions, the limited structural independence of the Data Protection Board, and the narrower rights catalogue compared to earlier drafts and the GDPR leave meaningful questions about how robustly the Act will, in practice, protect the informational privacy interests that Puttaswamy identified as constitutionally fundamental. With full operationalisation scheduled for May 2027, the coming years—and the content of further subordinate rules, Board jurisprudence, and any judicial review of the Act's exemption provisions—will determine whether the DPDP Act fulfils its constitutional mandate or merely formalizes a compliance regime around it.

References

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

The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), Gazette of India.

The Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, notified 13 November 2025.

Ministry of Electronics and Information Technology, Government of India. (2025). Press Note on Notification of the DPDP Rules, 2025.

Report of the Committee of Experts on Data Protection Framework for India (Justice B.N. Srikrishna Committee), 2018.

Regulation (EU) 2016/679 (General Data Protection Regulation).

Joint Parliamentary Committee Report on the Personal Data Protection Bill, 2019 (2021), Lok Sabha Secretariat.

Various law-firm and industry analyses of the DPDP Rules, 2025 implementation timeline (Lexology, Bar & Bench, 2025–2026).