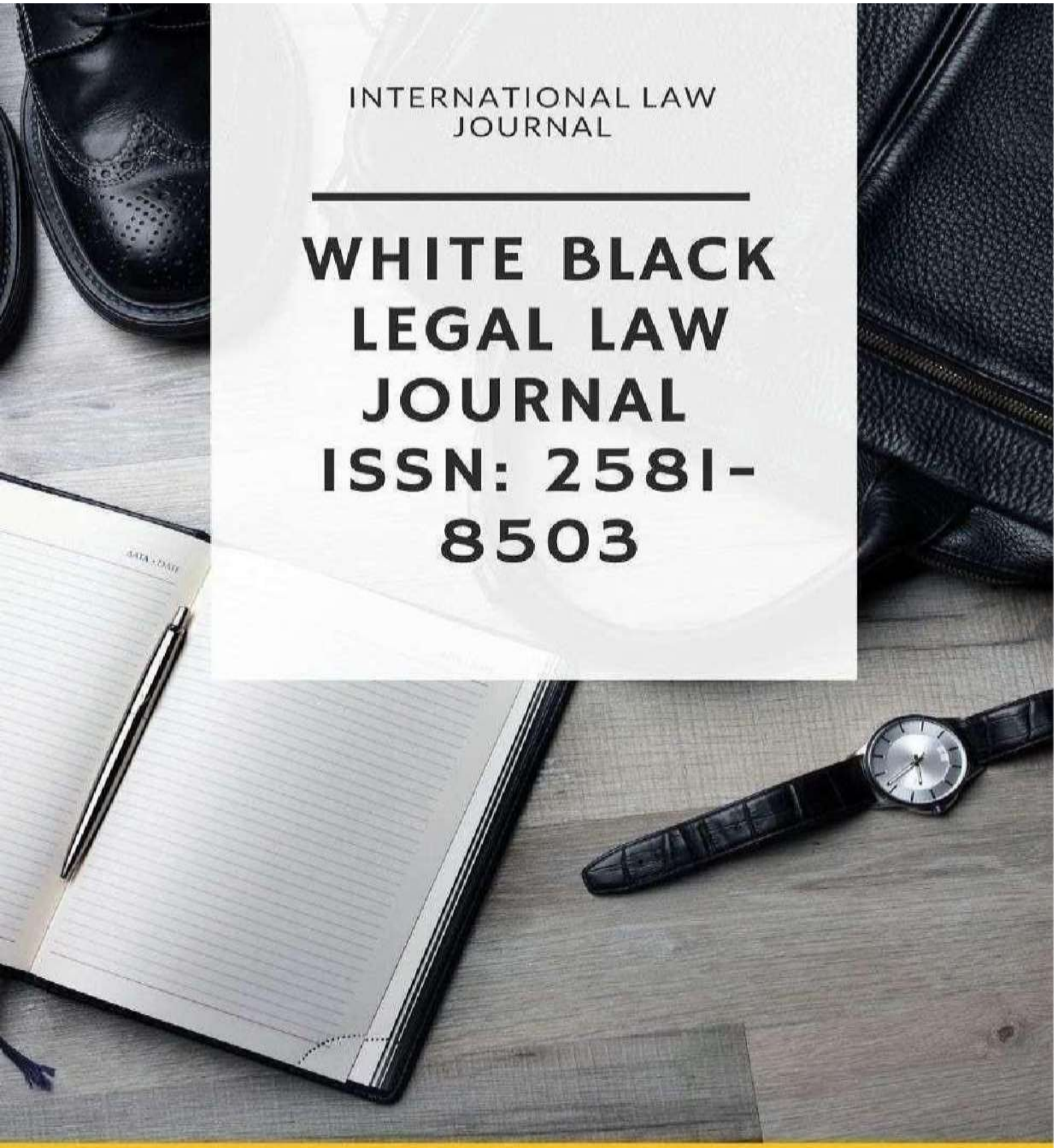

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

"THE PRICE OF PRIVACY: A CRITICAL ANALYSIS OF CORPORATE AND STARTUP COMPLIANCE OBLIGATIONS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023"

AUTHORED BY – ADV. SHIVRAJ PHALKE
CO – AUTHOR -PROF.RAHI AJABE - ALHAT
CLASS – LLM Business Law
COLLEGE – VISHVAKARMA UNIVERSITY PUNE

ABSTRACT

The enactment of the Digital Personal Data Protection Act, 2023 represents a watershed moment in Indian legal history, translating the fundamental right to privacy recognised by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* into a comprehensive statutory framework for the governance of personal data. While the Act is celebrated as India's most significant legislative intervention in digital governance, it simultaneously imposes a tripartite compliance architecture on corporations and start-up encompassing stringent consent and notice obligations, mandatory data breach notification requirements, and restrictions on cross-border data transfers the workability, proportionality, and coherence of which remain subjects of considerable legal and regulatory uncertainty. This paper undertakes a doctrinal and analytical examination of these three compliance domains, interrogating whether the Act's obligations are calibrated to the operational realities of India's heterogeneous digital economy, whether the penalty regime is proportionate in its impact on entities of varying scale, and whether certain State exemptions under Section 17 survive the constitutional scrutiny mandated by the Puttaswamy proportionality test. The paper concludes with reform recommendations directed at policymakers, advocating for a tiered compliance architecture that preserves robust data principal rights while fostering a regulatory environment conducive to digital innovation.

KEYWORDS

Digital Personal Data Protection Act 2023, Data Fiduciary, Consent Architecture, Data Breach Notification, Cross-Border Data Transfer

INTRODUCTION

Data has emerged as the defining economic resource of the twenty-first century. In India - a nation home to over 820 million internet users[1] and one of the world's three largest startup ecosystems[2]- the governance of personal data sits at the nexus of fundamental rights, economic policy, and sovereign interest. For decades, Indian data governance operated through the patchwork regime of the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 instruments widely criticised for their inadequacy, limited enforceability, and failure to account for the architectural transformation of the digital economy since their enactment.[3]

The watershed came not from Parliament but from the Supreme Court. In the landmark nine-judge bench decision of *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Court unanimously recognised the right to privacy as a fundamental right under Article 21 of the Constitution of India.[4] Justice D.Y. Chandrachud, in his concurring opinion, elaborated informational privacy as a distinct dimension of that right - the individual's autonomy over the collection, storage, and dissemination of their personal data. The decision placed a constitutional obligation on the legislature to enact a comprehensive data protection framework- a mandate that took six years, multiple draft Bills, and a joint parliamentary committee process to fulfil.

The Digital Personal Data Protection Act, 2023 (hereinafter "the DPDP Act" or "the Act") received Presidential assent on 11 August 2023, becoming India's first comprehensive personal data protection statute.[5] It establishes a rights-based framework governing the processing of digital personal data, creates the roles of Data Fiduciaries and Consent Managers, and establishes the Data Protection Board of India as the primary enforcement authority.

Yet the celebration of this legislative achievement must be tempered by rigorous scrutiny. The DPDP Act imposes substantial compliance obligations on all entities that process personal data of Indian citizens-obligations that, while defensible in principle, raise serious questions of

[1]Telecom Regulatory Authority of India, 'Telecom Subscription Data' (Annual Report 2024–25), available at <https://www.trai.gov.in (last visited on May 25, 2026). The figure represents active internet subscribers.
[2]India is widely recognised as one of the world's three largest start -up ecosystems by number of unicorns and funded ventures. See NASSCOM, 'India Tech Trends Report 2024–25' (2025). Figures are subject to variation by methodology and reporting period.
[3]Justice B.N. Srikrishna Committee, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (Ministry of Electronics and Information Technology, Government of India, 2018) pp. 3–7.
[4]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[5]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023). The Act received Presidential assent on 11 August 2023 and was published in the Gazette of India Extraordinary on that date.

workability, proportionality, and coherence in practice. Three compliance domains stand out in their significance for corporations and start-ups: the consent and notice architecture under Sections 5 and 6; the data breach notification obligations and penalty framework under Section 8(6) and the Schedule; and the cross-border data transfer restrictions under Section 16. These three domains collectively constitute what this paper describes as the "compliance trilemma" of the DPDP Act.

This paper undertakes a doctrinal and analytical examination of these domains, grounded in constitutional jurisprudence and assessed against the operational realities of India's corporate and start up landscape. The methodology is doctrinal drawing on statutory interpretation, constitutional adjudication, and analytical engagement with the legislative design - supplemented by comparative reference to the General Data Protection Regulation of the European Union, which has emerged as the international benchmark for comprehensive data protection law. The paper also briefly interrogates whether the State exemptions under Section 17 are constitutionally sustainable against the proportionality standard established in *Puttaswamy*. The central thesis is that the DPDP Act, while constitutionally necessary and directionally sound, imposes a compliance burden that is disproportionately onerous for smaller enterprises, lacks adequate regulatory clarity in critical areas, and contains structural gaps that require urgent legislative and regulatory attention.

THE CONSTITUTIONAL MANDATE AND THE LEGISLATIVE ARCHITECTURE

The constitutional prehistory of the DPDP Act is inseparable from the evolution of privacy jurisprudence in India. For much of post-independence constitutional law, privacy occupied an uncertain position acknowledged as a social value but never unequivocally recognised as a fundamental right. The eight-judge bench in *M.P. Sharma v. Satish Chandra*[6] declined to recognise a constitutional right to privacy, and the judgment in *Kharak Singh v. State of Uttar Pradesh*[7] produced a fractured outcome in which only a minority endorsed a limited privacy right. It was not until *Gobind v. State of Madhya Pradesh*[8] that a limited right to privacy was acknowledged as emanating from Articles 19 and 21 - a recognition immediately qualified by the observation that it was subject to compelling state interest.

The nine-judge bench in *Puttaswamy* definitively resolved this constitutional uncertainty.

[6]M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
[7]Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
[8]Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.

Privacy was declared a fundamental right - not a legislative concession but an intrinsic attribute of human dignity and autonomy, incapable of being abrogated by any State action that did not satisfy the requirements of constitutionality. Justice D.Y.Chandrachud's concurrence offered the most elaborate treatment of informational privacy: the right of an individual to control information about themselves constituted a protected dimension of the right to life and personal liberty under Article 21. Crucially, the Court articulated a three-part proportionality test for any permissible interference with privacy: first, the existence of a law authorising the interference; second, the pursuit of a legitimate State aim; and third, proportionality between the means employed and the aim pursued a requirement that the interference be necessary and not excessive relative to its objective.[9]

The legislative response to *Puttaswamy* was neither immediate nor straightforward. The Justice B.N. Srikrishna Committee submitted its report and draft Personal Data Protection Bill in July 2018, proposing a consent-first framework with limited non-consensual processing grounds and robust institutional oversight through an independent data protection authority. The Personal Data Protection Bill, 2019, referred to a Joint Parliamentary Committee, was ultimately withdrawn in August 2022. A leaner Digital Personal Data Protection Bill was released for public consultation in November 2022, and the resulting DPDP Act of 2023 reflected significant departures from the Srikrishna framework: it dispensed with an independent data protection authority in favour of a Government-constituted Board, substantially simplified the rights architecture, and adopted a more permissive approach to State exemptions. These departures carry constitutional and regulatory implications that this paper examines across its analytical sections.

The Act is structured around a consent-centric model for the lawful processing of digital personal data. The Data Fiduciary any person who alone or in conjunction with others determines the purpose and means of processing personal data may process such data only on the basis of the Data Principal's consent under Section 6 or one of the specified "legitimate uses" permitted without consent under Section 7. The Act further designates certain entities as Significant Data Fiduciaries under Section 10 identified by the Central Government on the basis of the volume and sensitivity of data processed, potential risk to Data Principal rights, and implications for national security and sovereignty. Significant Data Fiduciaries attract enhanced obligations, including appointment of a Data Protection Officer, engagement of an

[9]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, per Chandrachud J. (as he then was), concurring. The learned Judge identified legality, legitimate aim, and proportionality as the three-limb test for constitutionally permissible interference with the right to privacy.

independent data auditor, and periodic data protection impact assessments. It is this layered architecture sound in design but demanding in execution that forms the subject of the analysis that follows.

THE CONSENT ARCHITECTURE — OBLIGATIONS, AMBIGUITIES, AND CORPORATE COMPLIANCE BURDENS

The consent architecture of the DPDP Act represents one of its most operationally significant and demanding compliance domains. Section 6(1) stipulates that a Data Fiduciary may process personal data only if the Data Principal has given consent that is "free, specific, informed, unconditional and unambiguous," constituting a "clear affirmative action." Prior to seeking consent, Section 5 requires the Data Fiduciary to give the Data Principal a notice in plain language, in English or a language specified in the Eighth Schedule to the Constitution itemising the personal data sought to be processed, the purpose of processing, and the manner in which the Data Principal may exercise the right to withdraw consent or lodge a grievance.

The surface elegance of this framework is undeniable. The DPDP Act's consent standard broadly mirrors the requirements of the GDPR under Article 7, which similarly demands that consent be freely given, specific, informed, and unambiguous.[10] However, the Act diverges from the GDPR in several structurally significant ways that bear directly on the corporate compliance obligation, and in particular on the capacity of smaller enterprises to build sustainable consent architectures.

The first compliance challenge is one of granularity. The requirement that consent be "specific" carries the implication that a single omnibus consent covering multiple unrelated processing purposes is impermissible a conclusion reinforced by the requirement that the notice identify each purpose of processing. For a corporation operating a digital platform across multiple verticals marketing analytics, service personalisation, fraud detection, and third-party data sharing the obligation to obtain purpose specific consent for each processing activity, documented and audit ready, demands a consent management infrastructure of considerable complexity and cost. Unlike the GDPR, which is supplemented by extensive regulatory guidance from the European Data Protection Board on layered privacy notices and granular consent mechanisms, the DPDP Act offers no equivalent regulatory elaboration. The content of compliant consent practices awaits the notification of Rules under Section 40, creating a

[10]General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Article 7 read with Recitals 32 and 42.

period of compliance indeterminacy that exposes Data Fiduciaries to legal uncertainty in their daily operational decision-making.

The second compliance challenge is the language obligation. Section 5's requirement that the notice be provided in English or any Eighth Schedule language implies, for consumer-facing platforms with large and linguistically heterogeneous user bases, an obligation to maintain and update consent notices across potentially twenty-two constitutional languages. The operational overhead of professional legal translation, quality control, and notice synchronisation across linguistic versions constitutes a significant and recurring compliance cost one that falls disproportionately on smaller platforms that lack established localisation operations and dedicated legal compliance teams.

The third challenge concerns consent withdrawal. Under Section 6(4), a Data Principal may withdraw consent at any time, and the Data Fiduciary must cease processing "as soon as it is reasonably practicable." This formulation, while nominally flexible, is legally unsatisfying in an automated data environment where processing occurs continuously and algorithmically. The absence of a defined maximum period for ceasing processing following withdrawal creates uncertainty for both Data Principals seeking to exercise their rights and Data Fiduciaries seeking to build compliant systems with deterministic obligations.

Section 6(9) of the Act introduces the Consent Manager a registered intermediary through whom a Data Principal may give, manage, review, and withdraw consent to one or more Data Fiduciaries. The Consent Manager framework holds considerable promise as a structural solution to the fragmentation inherent in a consent-centric regime. However, its operationalisation is entirely contingent on Rules that, at the time of writing, have not been notified. The criteria for Consent Manager registration, their liability framework, and their technical interoperability requirements remain unspecified. Until these Rules are issued, the Consent Manager is an architectural feature of the Act that exists in name only a design aspiration awaiting regulatory substance.

The consent compliance burden falls with particular severity on start ups and small enterprises. A fintech, ed tech, or health tech start up may process multiple categories of personal data for several distinct purposes within a single product. Building a consent management infrastructure that is granular, multilingual, auditable, and capable of processing real-time withdrawals requires both technical resources and specialised legal expertise that are routinely beyond the reach of a seed-stage or early-growth entity. The DPDP Act, by applying identical consent obligations to a twenty-person start up and a Fortune 500 platform corporation, exhibits a structural indifference to enterprise scale that is a material legislative shortcoming. The absence

of a tiered compliance framework that calibrates the intensity of consent obligations to the volume, sensitivity, and risk profile of data processed is perhaps the single most significant regulatory design failure of the Act from a start ups ecosystem perspective.

DATA BREACH NOTIFICATION AND THE PENALTY REGIME — ACCOUNTABILITY OR OVERCORRECTION?

Section 8(5) of the DPDP Act imposes on every Data Fiduciary a duty to protect personal data by implementing "reasonable security safeguards to prevent personal data breach." Section 8(6) further provides that upon the occurrence of a personal data breach, the Data Fiduciary shall notify the Data Protection Board and each affected Data Principal "in such form and manner as may be prescribed." The structural gap in this provision is conspicuous: neither the timeline for breach notification nor the minimum content of the notification is specified in the Act itself. Both are deferred to subordinate Rules. This stands in sharp contrast to the GDPR's Article 33, which mandates notification to the supervisory authority within seventy-two hours of becoming aware of a breach.[11] The absence of a statutory notification timeline even a default maximum period leaves Data Fiduciaries unable to embed breach response protocols into their operational playbooks with any legal certainty. This is not a minor oversight; breach response timelines directly determine the readiness of incident response teams, the structure of regulatory insurance products, and the content of contractual breach notification clauses between Data Fiduciaries and their processors.

The Data Protection Board of India, constituted under Section 19 of the Act, is the primary enforcement authority. The Board is empowered to inquire into personal data breaches, determine compliance failures, and impose financial penalties. It operates as a digital-first adjudicatory body, conducting proceedings electronically. However, the Board's composition and appointment mechanism have attracted scholarly scrutiny on grounds of institutional independence. The Board's Chairperson and members are appointed by the Central Government on the recommendation of a Search-cum-Selection Committee the same authority that retains extensive exemption powers under Section 17 and the power to issue directions to the Board in specified circumstances. The creation of an enforcement body structurally tethered to the executive, tasked with enforcing an Act from which the executive can exempt its own instrumentalities, represents a governance arrangement that is at best constitutionally

[11]GDPR, Article 33(1): 'the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.'

inconvenient and at worst incompatible with the independence imperatives of rights adjudication.

The Schedule to the DPDP Act establishes a financial penalty framework of significant deterrent ambition. Failure to implement adequate security safeguards in contravention of Section 8(5) attracts a penalty of up to two hundred and fifty crore rupees. Failure to notify a breach under Section 8(6) attracts a penalty of up to two hundred crore rupees. Non-fulfilment of obligations regarding children's data under Section 9 and of additional Significant Data Fiduciary obligations under Section 10 each attract penalties of up to two hundred crore rupees. These figures are striking, and deliberately so they signal a legislative intent to make data protection violations economically consequential for large platforms.

However, the penalty structure raises serious proportionality concerns when applied to the broader universe of Data Fiduciaries. The Schedule prescribes maximum quantum figures without calibrating them to the size, revenue, or processing scale of the offending entity. A penalty of two hundred and fifty crore rupees represents a manageable regulatory expense for a multinational technology corporation and a liquidating liability for a start up with a total valuation below that threshold. The GDPR's penalty framework, by contrast, sets its upper limit as a proportion of global annual turnover up to four percent of worldwide annual turnover under Article 83(5)[12] thereby ensuring that the sanction bears a structural relationship to the offender's economic scale. India's flat cap model lacks this proportionality anchor, and in the absence of Rules prescribing the factors relevant to penalty quantification, the penalty regime offers minimal guidance for proportionate enforcement.

A further legislative gap is the absence of a statutory safe harbour for entities that detect, self-report, and proactively remediate a personal data breach. International practice treats voluntary disclosure, prompt notification, and remedial action as significant mitigating factors in penalty assessment, creating constructive incentives for transparency and cooperation. The DPDP Act's silence on this dimension is a missed opportunity to align enforcement incentives with the values of accountability and transparency that the Act ostensibly promotes. It bears noting that the proportionality of the legislative design must itself be assessed against the standard articulated in *Puttaswamy*,[13] and a penalty regime that applies uniform financial caps irrespective of the offender's scale and the gravity of harm caused risks constituting a

[12]GDPR, Article 83(5). The maximum penalty of four percent of global annual turnover applies to the most serious categories of infringement including breach of basic processing principles and conditions for consent.

[13]Puttaswamy, supra fn. 9. The proportionality standard has been further elaborated in Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar Case), (2019) 1 SCC 1.

disproportionate instrument achieving the legitimate aim of data protection through means that are excessive relative to that aim when applied to smaller entities.

CROSS-BORDER DATA TRANSFER RESTRICTIONS — SECTION 16 AND ITS COMMERCIAL IMPLICATIONS

Cross-border data transfer sits at the intersection of data sovereignty, trade policy, and corporate operational necessity. Section 16(1) of the DPDP Act provides that the Central Government may, after such consultation as it considers necessary, notify countries or territories to which a Data Fiduciary may transfer personal data outside India. This "whitelist" model under which transfers are permitted only to affirmatively notified jurisdictions represents a significant departure from the Personal Data Protection Bill, 2019, which contemplated a combination of adequacy assessments, contractual safeguards, and consent-based mechanisms.[14] The Act's streamlined model trades regulatory complexity for executive flexibility, with attendant costs for legal certainty.

As of the date of writing, no notification identifying permitted countries under Section 16 has been issued by the Central Government. The Act has therefore created a cross-border transfer regime that is architecturally complete but operationally empty a legal framework awaiting the regulatory content that would make it actionable. In the interim, Data Fiduciaries have no legal basis for determining which cross-border transfers are permissible, and no alternative legal mechanism is available to authorise transfers pending country notification.

For multinational corporations, the implications are substantial. Cross-border data flows are not incidental operations but architectural necessities: cloud computing services, international payroll processing, customer relationship management platforms, global analytics pipelines, and data backup and disaster recovery systems routinely involve the transfer of personal data of Indian citizens to servers or processors located outside India. The regulatory uncertainty created by the absence of notified countries renders vendor due diligence, data processing agreement drafting, and compliance risk assessment structurally incomplete. These are not abstract compliance inconveniences; they directly impair the legal enforceability of data transfer contracts and the accuracy of data protection representations made to regulators and customers.

For Indian start ups, the impact is differently constituted but equally material. India's start-up

[14]Srikrishna Committee Report (2018), Chapter 9 ('Cross-Border Transfer of Personal Data') pp. 93–100. The Committee proposed a hybrid model combining adequacy assessments, contractual mechanisms, and intra-group transfer arrangements.

ecosystem is deeply integrated into the global technology stack SaaS companies process customer data on cloud infrastructure deployed internationally; BPO and ITES enterprises transfer client data to offshore processing centres as a matter of operational design; and globally-aspirant product companies maintain data infrastructure across jurisdictions for latency optimisation, redundancy, and market penetration. The compliance obligation around cross-border transfers, whose concrete content remains unknown pending country notification, leaves start -up founders and their legal advisors unable to make informed decisions about data architecture investments at a stage when those decisions carry multi-year strategic consequences.

The GDPR's approach to cross-border transfers provides more operationally workable framework by comparison. Under Chapter V of the GDPR, transfers may be effected on the basis of an adequacy decision, appropriate safeguards including Standard Contractual Clauses and Binding Corporate Rules, or derogations for specific situations. The existence of Standard Contractual Clauses as a widely deployed and legally certain transfer mechanism has been particularly significant for smaller enterprises that lack the resources to negotiate bespoke data transfer arrangements. The DPDP Act provides for none of these alternative mechanisms. Its binary structure transfers permitted to notified countries, transfers to non-notified countries impermissible offers no contractual safeguard pathway and no adequacy assessment mechanism accessible to private parties.

It is important to engage candidly with the policy rationale for the Section 16 framework. India's debate on data localisation and cross-border transfer restrictions has been driven by legitimate concerns about regulatory access to data held by foreign entities, national security, and the economic case for processing Indian data within Indian jurisdiction. These are genuine sovereign interests that can, in principle, satisfy the legitimate aim component of the *Puttaswamy* proportionality test. The question is whether a blanket whitelist model with no interim transfer mechanisms, no timeline for country notifications, and no alternative legal pathways — is a proportionate means of achieving those ends, or whether it overcorrects in a manner that imposes unreasonable commercial burdens without commensurate data protection gains.

STATE EXEMPTIONS, CRITICAL ASSESSMENT, AND REFORM RECOMMENDATIONS

Section 17 of the DPDP Act empowers the Central Government to exempt specific data fiduciaries or classes of data fiduciaries from the application of all or any of the Act's provisions, including for purposes of national security, public order, and the prevention and detection of offences. The width of this exemption is constitutionally significant. Assessed against the three-part proportionality test from *Puttaswamy*, the exemption satisfies the legality requirement it is created by statute. The pursuit of national security and public order are legitimate state aims. The proportionality question, however, is acute: Section 17 creates an open-ended exemption covering an unlimited range of government data processing activities without requiring the Government to demonstrate necessity in any particular case, and without providing for independent judicial or parliamentary oversight. An exemption that removes entire categories of State data processing from the Act's privacy protections - including consent obligations, data principal rights, and breach notification requirements - without a necessity requirement or oversight mechanism risks creating the very privacy-free zone for State actors that the *Puttaswamy* Court sought to constitutionally foreclose. This concern is amplified by the structural dependence of the Data Protection Board on the executive, examined in the preceding section.

The analysis of the DPDP Act's tripartite compliance architecture reveals three systemic weaknesses that collectively constitute the compliance challenge examined in this paper. The first is regulatory incompleteness: the Act's practical effectiveness is substantially contingent on the notification of subordinate Rules under Section 40, and critical compliance parameters - including breach notification timelines, Consent Manager registration criteria, cross-border transfer country lists, and factors for penalty quantification - remain unnotified, creating a condition of compliance indeterminacy that falls most heavily on smaller entities. The second is scalar indifference the Act applies consent, security safeguard, and penalty obligations uniformly to all Data Fiduciaries regardless of size, resource capacity, and risk profile, without a tiered compliance framework that calibrates obligations to enterprise scale. The third is cross-border ambiguity: Section 16 creates a legally sound but operationally inert framework pending country notification, with no interim transfer mechanisms to bridge the operational gap.

From this analysis, five reform recommendations emerge. First, the Ministry of Electronics and Information Technology should prioritise notification of Rules under Section 40 with a publicly announced and binding timeline, giving particular urgency to breach notification timelines and

the cross-border transfer country list. Second, the DPDP Act should be supplemented by Rules introducing a tiered compliance framework that reduces the intensity of consent and documentation obligations for Data Fiduciaries below a prescribed threshold of data processing volume or annual turnover. Third, the penalty framework should be reformed to incorporate a revenue-linked penalty cap alongside the flat-cap model, ensuring that sanction quantum bears a structural relationship to the offender's economic scale. Fourth, the Central Government should introduce alternative cross-border transfer mechanisms - including model contractual clauses and provisional adequacy assessments - to bridge the operational gap until the country notification regime matures. Fifth, the State exemptions under Section 17 should be narrowed and subjected to a statutory necessity requirement and independent judicial oversight, to ensure consistency with the proportionality standard established in *Puttaswamy*.

CONCLUSION

The Digital Personal Data Protection Act, 2023 occupies a position of genuine historical significance in Indian legal history. It translates a constitutional mandate into statutory form, creates a new institutional architecture for data protection enforcement, and signals India's entry into the global data governance conversation after years of legislative delay. These are accomplishments that should not be minimised by the scholar's critical gaze.

And yet the rigorous examination of the Act's compliance architecture the consent framework, the breach notification and penalty regime, and the cross-border transfer structure reveals a statute that is structurally ambitious but operationally incomplete, constitutionally grounded but regulatorily underprepared. The compliance burden imposed by these three domains falls with disproportionate severity on start -ups and smaller enterprises precisely at the moment when India's digital economy most urgently needs those actors to innovate, scale, and compete globally.

The *Puttaswamy* Court recognised that the right to privacy could not exist in isolation from other constitutional values, and that permissible interference with privacy must satisfy the demands of proportionality. The DPDP Act's design, in its current form, does not fully honour that proportionality mandate - not because it protects too much, but because it calibrates too bluntly. A legal instrument that protects the rights of Data Principals while crushing the compliance capacity of innovative enterprises is not a well-designed privacy law. It is an instrument of regulatory burden that may ultimately undermine both the economic vitality and the rights culture it seeks to serve.

The corrections required are not radical. They are the corrections of operationalisation: notify the Rules, tier the compliance obligations, link the penalties to scale, provide cross-border transfer mechanisms, and narrow the State exemptions. India's digital economy, its startup ecosystem, and the data protection rights of its over 820 million internet users deserve a privacy law that is both robustly protective and sensibly calibrated. The price of privacy should not be the price of innovation.

REFERENCES

A. BOOKS

H.M. Seervai, Constitutional Law of India (Universal Law Publishing, New Delhi, 4th edn., 2010).

M.P. Jain, Indian Constitutional Law (LexisNexis, New Delhi, 8th edn., 2018).

Justice B.N. Shrikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indian - Report of the Committee of Experts on a Data Protection Framework for India (Ministry of Electronics and Information Technology, Government of India, 2018).

B. JOURNAL ARTICLES

Vrinda Bhandari & Renuka Sane, 'Towards a Privacy Framework for India in the Age of the Internet' (National Institute of Public Finance and Policy, Working Paper No. 2016-168, 2016).

Usha Ramanathan, 'A Unique Identity Bill' (2010) 45(35) Economic and Political Weekly 10.

C. STATUTES AND INTERNATIONAL INSTRUMENTS

The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

The Information Technology Act, 2000 (Act 21 of 2000).

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

The Constitution of India, 1950.

General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016.

California Consumer Privacy Act, Cal. Civ. Code § 1798.100 (2018, as amended by the California Privacy Rights Act, 2020).

D. WEBSITES

Ministry of Electronics and Information Technology, 'Digital Personal Data Protection Act, 2023', available at <https://www.meity.gov.in/data-protection-framework> (last visited on May 25, 2026).

Justice B.N. Srikrishna Committee, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (2018), available at <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> (last visited on May 25, 2026).

European Commission, 'Adequacy Decisions under GDPR', available at <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> (last visited on May 25, 2026).

European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (Version 1.1, 4 May 2020), available at <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> (last visited on May 25, 2026).