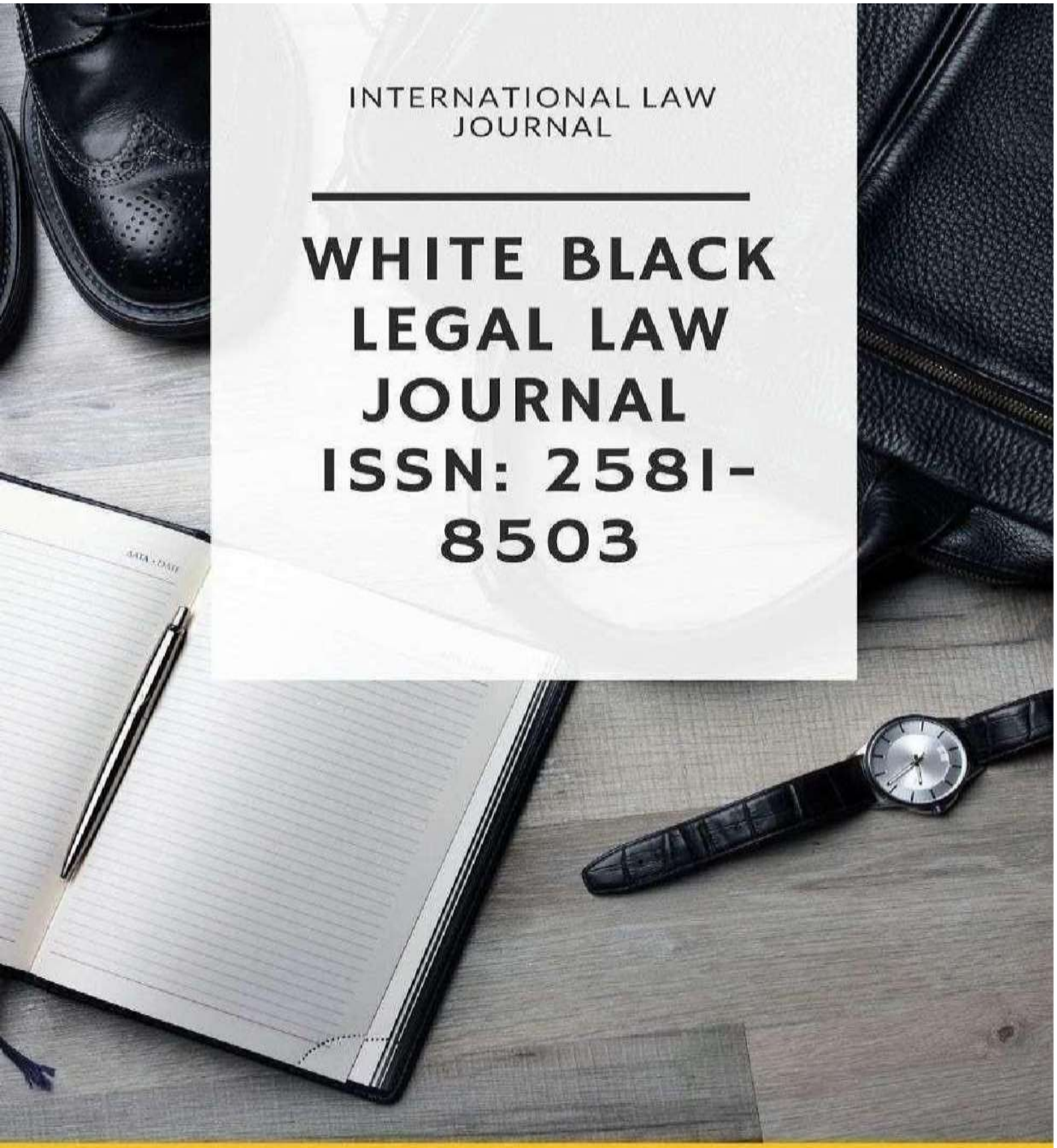

INTERNATIONAL LAW JOURNAL

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

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

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.

DATA PRIVACY COMPLIANCE AS A CORPORATE GOVERNANCE FUNCTION: THE IMPACT OF INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AUTHORED BY - AGAM RAVINDER LAMBA
BBA. LLB (H) (Corporate Law)
Amity Law School, Amity University, Noida

Abstract

The enactment of India's Digital Personal Data Protection Act, 2023 (DPDP Act) represents a watershed moment in the country's regulatory evolution. For the first time, Indian law provides a structured, rights-based framework governing the collection, processing, and protection of digital personal data. While most early commentary has focused on its compliance dimensions—notice obligations, consent mechanisms, penalty provisions—this article argues that the DPDP Act carries a deeper institutional significance: it elevates data protection from a technical IT concern to a core function of corporate governance. Drawing on constitutional jurisprudence rooted in the Puttaswamy judgment, comparative analysis with the European General Data Protection Regulation (GDPR), and India's extant corporate governance architecture under the Companies Act, 2013 and SEBI's LODR Regulations, this study examines how boards of directors must now incorporate data governance into their strategic oversight responsibilities. The article further identifies structural gaps in existing governance frameworks and offers doctrinal and practical recommendations for achieving meaningful board-level accountability over personal data.

Keywords: *DPDP Act 2023, Corporate Governance, Data Fiduciary, Data Protection Board, Puttaswamy, GDPR, Board Accountability, Digital Privacy, Significant Data Fiduciary*

I. Introduction: When Data Became a Governance Concern

For most of its modern legal history, India approached data protection as a regulatory afterthought. The Information Technology Act, 2000 was drafted primarily to facilitate e-commerce and digital transactions; its data-related provisions were incidental, fragmented, and poorly enforced. Corporations collected vast quantities of personal information from their

customers, employees, and business partners, largely unchecked. The implicit assumption was that data handling was an IT function—something for system administrators and cybersecurity consultants, not the boardroom.

The DPDP Act, 2023 disrupts this assumption fundamentally. Receiving presidential assent on 11 August 2023, the Act introduces a comprehensive, consent-driven framework for the processing of digital personal data in India. It establishes the Data Protection Board of India as a quasi-judicial regulatory body, confers enforceable rights upon individuals whose data is processed, and imposes structured obligations on entities that collect or use that data. The penalties for non-compliance are substantial—up to INR 250 crore for a single violation—and the accountability norms are expressly designed to reach beyond operational teams to the entities themselves.

The ambition of the Act is not merely regulatory. Read alongside the constitutional foundations laid by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India, the DPDP Act signals that personal data is a constitutional matter, not merely a commercial one. When a corporation processes a citizen's health records, financial transactions, or biometric data, it is engaging with that individual's fundamental right to informational privacy. The implications for corporate governance are profound.

This article takes the position that data privacy compliance under the DPDP Act must be reconceptualised as a corporate governance function. Section II situates the Act within India's broader digital economy and the risks that accompany it. Section III traces the constitutional lineage of data protection from Puttaswamy to the DPDP Act. Section IV examines how the Act's obligations map onto governance structures. Section V assesses India's existing corporate governance architecture and its readiness to absorb these obligations. Section VI draws lessons from the GDPR and global enforcement practice. Section VII identifies gaps and offers recommendations. Section VIII concludes.

II. India's Digital Economy and the Stakes of Data Governance

The scale of India's digital transformation is difficult to overstate. As of 2023, India has over 850 million active internet users, making it the second-largest online population in the world. The Jan Dhan–Aadhaar–Mobile (JAM) trinity, the Unified Payments Interface (UPI), and the proliferation of low-cost smartphones have together brought hundreds of millions of previously unbanked or digitally excluded citizens into a data-generating economy. Every digital interaction—a payment, a search query, a healthcare appointment, a social media post—

generates data points that are collected, stored, analyzed, and monetized.

Yet the speed of this transformation has not been matched by an equivalent maturation of data protection norms or corporate accountability. India has witnessed a succession of significant data breaches in recent years that illustrate the scale of the governance deficit. The 2018 Aadhaar breach exposed details of over one billion individuals. The 2021 MobiKwik breach allegedly compromised the data of approximately 99 million users. Air India's breach in the same year affected the sensitive passport and credit card information of 4.5 million passengers. More recently, the 2024 Star Health breach saw the data of approximately 31 million policyholders reportedly leaked through a Telegram bot, while a breach at BSNL in the same year exposed sensitive employee and subscriber records.

These breaches are not simply IT failures. They reflect failures of institutional governance—of risk oversight, of investment prioritization, and of accountability at the highest levels of organizations. When a company suffers a breach affecting millions of individuals, the question that regulators and shareholders should be asking is not only whether the technical defenses were adequate, but whether the board was informed of data-related risks, whether it directed appropriate resources toward managing those risks, and whether adequate escalation and reporting mechanisms were in place.

Data governance, in this sense, is inseparable from good corporate governance. Trust in digital services is a public good, and corporations that hold vast quantities of personal data are stewards of that trust. The DPDP Act gives legal expression to this principle.

III. The Constitutional Foundations: Puttaswamy and the Right to Informational Privacy

The DPDP Act does not emerge from a legislative vacuum. Its constitutional antecedents trace directly to the nine-judge bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, one of the most consequential constitutional rulings in India's legal history.

The Court, speaking with remarkable unanimity across six separate concurring opinions, held that the right to privacy is a fundamental right guaranteed under Articles 14, 19, and 21 of the Constitution of India. The judgment was not merely declaratory; it was architecturally significant. It situated privacy within the framework of human dignity and autonomy, recognizing that control over one's personal information is central to the exercise of individual freedom in a modern democratic society.

Of particular relevance for corporate compliance is the Court's recognition of informational

privacy as a protected dimension of the right to privacy. The Court articulated that individuals have a right to control the collection, use, and dissemination of their personal information. Importantly, the Court did not limit this right to state actors. While constitutional rights are classically understood as rights against the state, the reasoning in Puttaswamy—particularly in Justice D.Y. Chandrachud's concurring opinion—has been interpreted as extending the privacy norm to private actors who process personal data on a significant scale.

The Puttaswamy framework operates through a three-part test: any limitation on the right to privacy must be backed by law; it must pursue a legitimate state aim; and it must be proportionate to the harm sought to be prevented. Applied to corporations, this framework implies that data processing activities must have a lawful basis (consent, legitimate use, or another recognized ground), must serve a genuine and disclosed purpose, and must not collect or retain more data than is necessary for that purpose.

The DPDP Act operationalizes this constitutional principle through a statutory framework. Consent notices must be clear and specific; purposes must be disclosed at the point of collection; data must be erased once the purpose is served; and individuals must be empowered to enforce their rights through grievance mechanisms and, ultimately, through the Data Protection Board. The Act thus converts constitutional aspiration into enforceable legal obligation—and places corporations squarely within that obligation.

IV. The DPDP Act and the Architecture of Corporate Obligation

The DPDP Act's normative architecture organizes corporate obligations around two central concepts: The Data Fiduciary and the Significant Data Fiduciary. Understanding both is essential to appreciating why the Act demands governance-level engagement rather than mere compliance-level management.

4.1 The Data Fiduciary

Section 2(i) of the DPDP Act defines a Data Fiduciary as any person who, alone or in conjunction with other persons, determines the purpose and means of processing personal data. The term 'fiduciary' is not accidental. It consciously evokes a relationship of trust—an acknowledgment that the entity holding and processing personal data does so in a position of power relative to the individual, and must therefore discharge that power responsibly.

The obligations imposed on Data Fiduciaries under Sections 8 and 9 of the Act are consequential. A Data Fiduciary must: obtain free, informed, specific, and unconditional

consent before processing personal data; provide a clear and accessible notice at the point of consent; ensure the completeness, accuracy, and consistency of personal data; implement reasonable security safeguards proportionate to the nature and volume of data processed; notify the Data Protection Board and affected Data Principals of breaches without delay; erase personal data upon withdrawal of consent or once the purpose of processing is fulfilled; and establish a functioning grievance redressal mechanism.

Each of these obligations has structural implications. Consent management at scale requires investment in technology infrastructure, legal review, and policy design. Data accuracy obligations necessitate internal data quality processes. Breach notification demands incident response protocols that bridge technical teams and senior management within a defined window. Data erasure requires governance of the entire data lifecycle. None of these functions can be delegated entirely to IT teams; each demands strategic direction and resource commitment from the institutional leadership of the corporation.

4.2 The Significant Data Fiduciary

Section 10 of the DPDP Act introduces the category of the Significant Data Fiduciary (SDF). The Central Government may designate an entity as an SDF based on factors including the volume and sensitivity of data processed, the potential risk to the rights of Data Principals, national security implications, and the impact on democratic processes or the sovereignty of India.

SDFs carry a notably elevated compliance burden. They are required to appoint a Data Protection Officer (DPO) who must be a senior officer of the entity and who bears ultimate responsibility for compliance. They must conduct periodic Data Protection Impact Assessments (DPIAs) to identify and mitigate risks arising from their data processing activities. They must submit to independent audits by external auditors approved by the Board. And they must establish systems for algorithmic accountability, including the capacity to explain automated decisions that affect individuals.

Critically, the DPO of an SDF is not merely a compliance officer in the traditional sense. The Act envisages the DPO as a senior officer who reports directly to the board, advises the entity on its data protection obligations, and acts as the primary point of contact with the Data Protection Board. This design mirrors the approach of the GDPR, which requires that DPOs have expert knowledge of data protection law, operate with independence, and have direct access to the highest level of management. When a DPO reports to a board, data protection is no longer a functional concern—it becomes a governance one.

4.3 Rights of Data Principals and Corporate Duties

Chapter V of the DPDP Act Grants Data Principals a suite of enforceable rights: the right to access information about the nature, purpose, and scope of their data processing; the right to correction and erasure of personal data; the right to grievance redressal within defined timelines; and the right to nominate a representative to exercise these rights in the event of incapacity or death. These rights are not merely aspirational. They are backed by the enforcement powers of the Data Protection Board, which may impose penalties of up to INR 250 crore per violation and direct remedial action.

For corporations, honoring these rights requires more than a compliance checklist. It requires the construction of internal mechanisms—data mapping systems, request-handling workflows, escalation protocols, and legal review processes—that function consistently and at scale. Boards must be satisfied that these mechanisms are in place, adequately resourced, and tested. The board's duty of oversight, long recognized under corporate law, now extends unmistakably to data rights infrastructure.

V. India's Corporate Governance Framework and Its Data Readiness

India's corporate governance regime rests on two principal pillars: The Companies Act, 2013 and the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (LODR Regulations). These instruments, informed by successive governance reform committees—the Kumar Mangalam Birla Committee of 2000, the Narayana Murthy Committee of 2003, and more recent advisory bodies—have progressively strengthened board accountability, risk management obligations, and disclosure norms.

Section 166 of the Companies Act, 2013 requires directors to act in good faith and in the best interests of the company, its employees, shareholders, and the community. Section 134(3)(n) mandates that the Board's Report include a statement on the company's risk management policy, including the elements of risk that may threaten the company's existence. Regulation 17 of the LODR Regulations requires listed entities to constitute a board-level Risk Management Committee with at least three directors, and Regulation 21 mandates that listed entities having a net worth of INR 500 crore or a turnover of INR 1,000 crore formulate a risk management framework.

These provisions create an existing governance infrastructure that can, in principle, accommodate data-related risks. However, in practice, data governance remains inadequately integrated into the risk management frameworks of most Indian corporations. Annual reports

rarely address data risks in a substantive manner. Risk Management Committees seldom include members with meaningful expertise in data protection law or cybersecurity. Board-level discussions of data governance are episodic rather than structural.

The DPDP Act creates an urgent imperative to close this gap. The Act's obligations—particularly for SDFs—are not satisfied by annual audit exercises or one-time policy drafting. They require ongoing governance engagement: quarterly updates to the board on data protection compliance; integration of DPIAs into the approval process for new products, services, and data processing activities; board sign-off on breach notification decisions; and explicit inclusion of data governance metrics in enterprise risk reporting.

There is also a disclosure dimension. Investors, regulators, and increasingly, consumers, are beginning to regard data governance quality as a material factor in assessing corporate value and risk. The SEBI framework's existing disclosure provisions do not currently require explicit reporting on data protection frameworks, breach incidents, or DPDP Act compliance. This represents a significant gap that SEBI—and corporate boards proactively—should address.

VI. The GDPR as a Mirror: Global Lessons for Indian Boards

No discussion of the DPDP Act's governance implications is complete without reference to the European General Data Protection Regulation (GDPR), which came into force in May 2018 and has since become the global benchmark for data protection law. The DPDP Act's structural similarities to the GDPR—consent-based processing, data subject rights, a mandatory DPO for certain categories of entities, significant financial penalties—reflect deliberate legislative borrowing. The GDPR's five-year enforcement record offers invaluable lessons about how data protection obligations translate into governance practice.

The most important lesson is that regulators in mature data protection regimes regard governance failures as distinct and serious violations. Meta Platforms was fined €1.2 billion by the Irish Data Protection Commission in 2023—the largest GDPR penalty on record—not only for the transfer of personal data to the United States without adequate safeguards, but because the violation reflected a systemic and prolonged governance failure. Similarly, the Italian Data Protection Authority imposed a €10 million penalty on a major utility company for inadequate board oversight of data processing practices. These cases establish a clear precedent: where a board has failed to take reasonable steps to understand, manage, and oversee data risks, the resulting penalties are amplified by that failure of oversight.

The GDPR enforcement record also illustrates that the DPO role is substantive rather than

ceremonial. European supervisory authorities have sanctioned entities where DPOs lacked genuine independence, were impeded from accessing board-level discussions, or were assigned to roles that created conflicts of interest with their data protection obligations. The design of the DPO function under the DPDP Act—senior officer, board-reporting, independent—signals that Indian regulators are seeking a comparable level of substantive engagement.

There is, however, an important structural difference between the GDPR and the DPDP Act that Indian corporations should note. The GDPR's penalties are calibrated as a percentage of global annual turnover—up to four percent under Article 83(5)—making them inherently scalable to the size of the violating entity. The DPDP Act's penalty structure, while substantial in absolute terms, is capped at fixed amounts. This design choice, while politically pragmatic, may reduce the deterrent effect of the penalty framework for very large corporations. It also places a premium on the reputational and regulatory consequences of non-compliance, rather than purely financial ones.

VII. Identifying Gaps and Offering Recommendations

A candid assessment of the DPDP Act's governance framework reveals both promise and gap. On the positive side, the Act's recognition of a fiduciary relationship between Data Fiduciaries and Data Principals, the DPO requirement for SDFs, the DPIA obligation, and the independent audit mechanism all reflect a governance-conscious regulatory design. The DPDP Rules, 2025 have added further operational specificity, and the Act's anticipated full implementation by 2027 provides corporations with a defined transition horizon.

However, several structural gaps warrant attention. First, the Act does not explicitly mandate board-level engagement with data governance. Unlike the UK Corporate Governance Code, which expressly addresses cyber and data risk as a board responsibility, or the US Securities and Exchange Commission's 2023 rules requiring public companies to disclose material cybersecurity incidents and annually disclose their cybersecurity risk management and governance practices, the DPDP Act operates primarily at the entity level without specifying the internal governance mechanisms required to discharge its obligations. This creates a risk that compliance is treated as a legal and operational matter rather than a strategic governance one.

Second, the designation criteria for SDFs remain opaque. The Act grants the Central Government broad discretion to designate entities as SDFs based on factors that include national security considerations and the impact on democratic processes. While flexibility is

understandable in an early regulatory regime, the absence of clear thresholds creates uncertainty for corporations seeking to plan their governance investments. Regulatory guidance from MeitY clarifying expected designations would significantly assist corporate compliance planning.

Third, the Data Protection Board's institutional capacity remains an open question. The Board is constituted as a quasi-judicial body with adjudicatory powers, but its independence from executive influence, its resourcing, and its technical expertise will be critical determinants of its effectiveness. The GDPR's enforcement record demonstrates that the deterrent effect of data protection law depends heavily on a credible, well-resourced regulator prepared to take action against significant entities. Building that institutional credibility will be among the Board's most important early tasks.

On the basis of this analysis, the following recommendations are offered:

First, the SEBI LODR Regulations should be amended to require listed entities to include a dedicated section on data governance in their annual corporate governance reports. This section should address the board's oversight role, the entity's data governance framework, material data incidents in the reporting year, and the adequacy of data protection infrastructure. Such mandatory disclosure would create market incentives for genuine governance investment and allow investors to assess data-related risks.

Second, corporate boards should proactively integrate data governance into their risk governance frameworks, even ahead of full regulatory implementation. Risk Management Committees should include at least one member with expertise in data protection law or cybersecurity. DPIAs should be treated as a standard component of new product or service approval processes, analogous to legal due diligence reviews.

Third, MeitY should publish detailed guidance on SDF designation criteria and on the expected qualifications, responsibilities, and independence protections of the DPO role. Guidance of this kind—analogous to the Article 29 Working Party guidelines under the GDPR—would reduce regulatory uncertainty and assist corporations in making appropriately informed governance investments.

Fourth, consideration should be given to introducing director-level liability provisions into the DPDP Act or its implementing rules, modelled on the approach taken under Section 299 and Schedule IV of the Companies Act, which impose personal obligations on directors in respect of defined governance failures. Targeted director accountability would complement entity-level penalties and create a more powerful incentive for genuine board engagement with data

protection obligations.

VIII. Conclusion: Toward a Governance Paradigm for the Data Age

The Digital Personal Data Protection Act, 2023 is a landmark piece of legislation. It is the product of years of parliamentary deliberation, expert consultation, and constitutional evolution, and it reflects a recognition—overdue but welcome—that the informational sovereignty of Indian citizens deserves the protection of a comprehensive legal framework.

But the significance of the Act extends well beyond the creation of a regulatory framework for data protection compliance. By establishing the concept of the Data Fiduciary and by imposing obligations that require strategic oversight, resource allocation, and institutional accountability, the Act effectively situates data governance at the heart of corporate governance. Boards of directors can no longer regard personal data as the exclusive concern of technology teams or legal departments. Data is an institutional responsibility—one that implicates fiduciary duties, reputation, constitutional obligations, and long-term enterprise value.

The case studies examined in this article—Aadhaar, MobiKwik, Air India, Star Health, BSNL—illustrate that data breaches at scale are not merely IT incidents. They are governance failures. They reflect deficits in risk identification, in institutional investment, and in board-level accountability. The DPDP Act creates the legal framework to hold corporations accountable for those failures. How effectively that framework is enforced will depend on the institutional capacity of the Data Protection Board, the regulatory ambition of MeitY and SEBI, and—crucially—the willingness of corporate boards to take their data governance obligations seriously.

The GDPR's experience over five years of enforcement offers both encouragement and a cautionary note. Encouragement, because the regulation has demonstrably elevated data protection standards across thousands of organizations and has produced a growing body of enforcement jurisprudence that has clarified expectations. Caution, because the early years of GDPR enforcement revealed that many organizations treated compliance as a paper exercise, and that substantive board engagement with data governance remained the exception rather than the rule. India has the opportunity—and the obligation—to learn from that experience.

India's digital journey is still in its formative stages. The policy choices made now—by legislators, regulators, and corporate boards—will shape the kind of digital economy that emerges over the next decade. If data governance is embedded meaningfully into corporate governance, India has the potential to build a digital economy that is not only prosperous but

also trustworthy, accountable, and rights-respecting. The DPDP Act provides the legislative foundation. The governance architecture must now be built upon it.

References

1. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
2. Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India.
3. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
4. Companies Act, 2013 (Act No. 18 of 2013), Sections 134, 166.
5. Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, Regulations 17, 21.
6. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), [2016] OJ L 119/1.
7. Information Technology Act, 2000 (Act No. 21 of 2000), Sections 43A, 72A.
8. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
9. Irish Data Protection Commission, Decision against Meta Platforms Ireland Limited (2023), DPC Inquiry Reference: IN-20-1-1.
10. Garante per la Protezione dei Dati Personali (Italian Data Protection Authority), Order No. 77 of 11 March 2021.
11. Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 17 CFR Parts 229, 232, 239, 240, 249 (2023).
12. Kumar Mangalam Birla Committee Report on Corporate Governance, Securities and Exchange Board of India (2000).
13. N.R. Narayana Murthy Committee Report on Corporate Governance, Securities and Exchange Board of India (2003).
14. Srikrishna, B.N. (Chair), A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018), Ministry of Electronics and Information Technology.
15. Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, WP 243 rev.01 (2017).
16. Narayanan, A., 'India's Data Protection Journey: From SPDI Rules to DPDP Act' (2023) 15 Indian Journal of Law and Technology 42.

17. Raman, S. and Kaur, P., 'Board Accountability in the Age of Data Governance: Lessons from GDPR Enforcement for Indian Corporations' (2024) 19 Corporate Governance: An International Review 213.
18. Krishnaswamy, S., Privacy and the Constitution (Oxford University Press, 2020).
19. Singh, A., 'The Data Protection Board of India: Institutional Design and Regulatory Effectiveness' (2024) 31 National Law School of India Review 88.
20. Centre for Internet and Society, India's Data Breach Landscape: A Study of Major Incidents 2018–2024 (Bengaluru, 2024).