International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2026 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

Data Protection Compliance Challenges for Indian Corporations Under the Digital Personal Data Protection Act, 2023

Yuvraj Singh[a]

[a]Bharati Vidyapeeth (Deemed to be University), New Law College, Pune, India

Received 02 March 2026; Accepted 01April 2026; Published 04 April 2026

The data-driven business models have created a wave of exponential growth in the collection and utilisation of personal data; this has brought both a rise in importance and a concern associated with privacy, surveillance, and business responsibility. As a response to this concern created by the use of personal data in digital business models in India, a new law titled the Digital Personal Data Protection Act of 2023 has been introduced to address this concern comprehensively and to move away from a patchwork regime to a comprehensive regime on data protection in India.[1] The present study critically evaluates the data protection compliance difficulties of Indian corporates in light of the application of the Digital Personal Data Protection Act of 2023. The study analyses the legal obligations of data fiduciaries in dealing with consent, data security measures, and data breach notification obligations, and the increased obligations of significant Data Fiduciaries under this Act. The study also assesses the data protection compliance enforcement mechanism created by this Act in relation to the powers and discretion of the Data Protection Board and penalty provisions for corporates. The paper contends that while the Act is indeed a step forward for data protection law in India, there are numerous ambiguities/shortcomings which might create an obstruction to its efficacious implementation, especially for SMEs. The issues about this problem have been identified as challenges to its implementation. With its doctrinal/analytical

[1] Digital Personal Data Protection Act 2023

methodology, this paper examines how an apt balance can or has been made between privacy protections for individuals with regard to undertaking business in an easier manner with the implementation of this legislation. Finally, recommendations for amending these ambiguities to make its implementation result in data protection law as an obstruction to punitive actions for delinquent corporations/entrepreneurs are provided.

Keywords: *digital personal data protection, data fiduciaries, corporate compliance, data protection board, privacy law.*

INTRODUCTION

The growing digital economy has resulted in personal data being considered a precious economic resource for companies across industries. Companies are increasingly using personal data to improve efficiency, innovation, and consumer engagement. This increased corporate dependence on personal data has triggered concerns related to privacy, misuse of personal data, and responsibility on the part of corporations. The concerns have taken on constitutional dimensions in India after recognising a right to privacy as a fundamental right under Article 21 of the Indian Constitution, thus demanding a holistic legislative structure for data protection in India.[2]

For quite some years, data protection law within the Indian jurisdiction was regulated by a patchwork system of law, largely under the Information Technology Act, 2000, as well as its subsidiary legislation.[3] This often drew widespread criticism for its narrow coverage, weak enforcement structures, and its inability to address new business models being developed using data. The recent law on Data Protection under the Digital Personal Data Protection Act, 2023, marks an entirely new approach to data protection as a self-contained law with human-oriented regulatory structures to regulate personal data processing within Indian Territory. The Act introduces a structured compliance architecture, imposing statutory obligations on data fiduciaries while simultaneously recognising the legitimate interests of businesses in processing personal data.

Although the proposed Digital Personal Data Protection Act of 2023 attempts to achieve a balance between the privacy of the individual and the promotion of economic growth, the

[2] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1
[3] Information Technology Act 2000

effectiveness of this bill will largely depend on the ability of corporations to comply with it.[4] The proposed act casts a heavy burden of obligations with reference to consent requirements, notice obligations, data protection safeguards, obligations for reporting a breach of data protection obligations, and the responsibilities of the proposed Significant Data Fiduciaries.

The paper will critically evaluate the challenges that corporations in India are facing in terms of compliance under the Digital Personal Data Protection Act 2023. The paper will also determine whether there is a level of clarity and proportionality in the legislation on data governance, and whether potential threats to proper enactment arise from a lack of clarity in corporate law. The paper will also determine if the legislation succeeds in ensuring that corporations within India are responsible in their handling of ease of doing business within India. The paper will utilise a doctrinal and analytical method for analysis.

RESEARCH QUESTIONS AND HYPOTHESIS

1. Does the Digital Personal Data Protection Act 2023 offer a clear, proportionate, and workable framework of compliance for Indian corporations, or are the regulatory obligations difficult to implement?
2. What are the main principal compliance requirements of the Digital Personal Data Protection Act 2023 that affect corporations?
3. How do ambiguities in consent, notice obligations, and data fiduciary duties impact corporate compliance?
4. What is the impact of the enforcement procedure provided under the Act, especially the function of the Data Protection Board, on corporate accountability?
5. What are the challenges posed by small and medium enterprises to data protection compliance requirements?
6. Does the current system of penalties encourage responsible data governance, or does it overly burden compliance?

HYPOTHESIS

The Digital Personal Data Protection Act 2023 represents a progressive step towards strengthening data protection in India; however, ambiguities in statutory obligations, reliance

[4] Constitution of India 1950, art 21

on delegated legislation, and the cost-intensive nature of compliance pose significant challenges for Indian corporations, potentially undermining effective implementation.

EVOLUTION OF DATA PROTECTION LAW IN INDIA

The evolution of data protection regulations within the Indian legal framework is a gradual and reaction-based process that was triggered by the advancements of technology and judicial pronouncements on the topic of data and privacy. In fact, the Indian legal framework was without a specific data protection law and had a patchwork of legal provisions to address concerns of personal data.

Firstly, data protection issues were dealt with by the Information Technology Act of 2000, specifically by sections related to unrestricted access, data fraud, and cybercrimes. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011[5] tried to lay down some elementary protections by requiring consent, disclosure requirements, and security practices for sensitive personal data. The framework failed to be effective due to its restricted applicability, weak enforcement, and uncertainties related to corporate responsibilities, hence failing to be effective in the handling of big data by the corporate world.

There was a major shift triggered by the judicial acknowledgement of the right to privacy as one of the inherent rights flowing from the reasonable interpretation of Article 21of the Indian Constitution. This constitutional shift acknowledged the need for a comprehensive statute[6] that could adequately take into consideration the need to preserve the privacy of the citizens, as well as the states' and businesses' needs. In this respect, expert committee reports and drafts have been raised from time to time regarding the need for the DP and the proposed statute.

The coming into effect of the Digital Personal Data Protection Act, 2023, represents a shift away from the prior patchwork regime, as it not only establishes a stand-alone regime for the processing of personal data but also the first law on data protection that is rights-oriented and

[5] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011
[6] Justice BN Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018)

focuses on obligations among data fiduciaries, with a focus on a centrally enforced regime. This is a deliberate shift away from data regulation through a regime coupled with penal provisions.

While the Act represents a leap forward in the data protection landscape of India, its journey also ushers in a new regime of regulatory centralisation and increased corporate liability. In that process, some key questions remain: will Indian companies adjust well to a compliance-intensive environment, and will the legislative design adequately account for the varied capacities of businesses operating in the digital economy? This historical evolution forms the necessary backdrop for an assessment of the challenges in compliance under the current statutory regime.

CORPORATE OBLIGATIONS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

The Digital Personal Data Protection Act 2023 sets a compliance framework by making certain mandatory requirements for entities categorised as data fiduciaries. The requirements ensure that personal data is processed in a lawful, transparent, and secure way while also making corporations responsible for any abuse/ignorance of personal data. The compliance framework of this act shifts its focus from voluntary data protection to a mandatory one.[7]

One of the primary obligations imposed on corporations is to respect the obtaining of valid consent from the data subject. The Act states that the consent required is free, specific, informed, unconditional, and unambiguous, and this is to be accompanied by an express notice[8] stating the purposes of data processing. It appears that for commercial corporations, especially those operating by consent, complying with these principles would be quite an operational challenge for the current practice of doing business.[9]

Besides the consents stipulated in the Act, there are obligations regarding data protection safeguards. Corporations must put in place reasonable technical and organisational measures with a view to ensuring that there are no personal data breaches. The requirement does not only involve complying with reasonable safeguards for the sector or industry that one belongs to. It involves constant monitoring for risks together with internal corporate governance structures.

[7] Digital Personal Data Protection Act 2023, s 2(i)
[8] *Ibid* s 5
[9] *Ibid* s 6

The lack of precise statutory authority regarding what reasonable safeguards entail poses a challenge for corporations.[10]

The Act also has accountability requirements in case of breaches of personal data. The data fiduciaries are required to notify the Data Protection Board and data principals about the breach of data in accordance with a prescribed manner.[11] In the case of corporations, the detection and reporting of breaches in a timely manner requires that information systems for compliance be developed within the organisation. Non-compliance with these requirements can also invite heavy penalties, thereby increasing data risks in data processing operations.

One of the interesting consequences of the Act is its categorisation of certain entities as Significant Data Fiduciaries based on certain parameters related to the volume or sensitivity of certain data.[12] These entities are obliged to comply with stringent requirements related to, among other things, the appointment of a Data Protection Officer, conducting data protection impact assessments, and data protection audits. The above requirement, while emphasising accountability, also adds to the costs of compliance.[13]

On the whole, the corporate obligations that have been introduced by the Digital Personal Data Protection Act, 2023, are indicative of a regulatory framework that emphasises the need to emphasise the aspect of accountability. The wide-ranging nature of these obligations suggests that there are interpretive challenges associated with these obligations. The challenges associated with compliance are essential in determining the effectiveness of the Act.

COMPLIANCE CHALLENGES FOR INDIAN CORPORATIONS

Although a structured compliance framework is established through the Digital Personal Data Protection Act, 2023, there are certain challenges that Indian corporations encounter while implementing this act. Such challenges arise due to certain ambiguities and limitations of operations and capacities of the concerned entities when such entities operate within India's digital economy. There is a certain gap created between legislative issues and actual implementation.

[10] Digital Personal Data Protection Act 2023, s 8(5)
[11] *Ibid* s 8(6)
[12] *Ibid* s 10
[13] Justice BN Srikrishna Committee (n 6)

A major issue would be the consent architecture. Although the legislation lays down strict standards to qualify consent, the legislation does not lay down adequate assistance in the consent mechanism that ensures the consent of the users. The standard-form digital interface schemes used by business entities can cause difficulties for business entities in balancing efficiency and consent. There are no specific guidelines from the legislation regarding compliance. This causes difficulties for industries driven by data, such as e-commerce.

Compliance costs are also a major issue that small and medium-sized enterprises find challenging. In fact, the cost of incorporating measures for the security of data, data breach detection systems, and governance within an organisation can be quite high. It can create a significant burden for some of these business organisations. It is pertinent to note that the Act does not address differences in compliance costs according to the size of the business.[14]

The process of cross-border data processing also causes difficulties from the perspective of compliance. Many Indian companies have a global reach and hence can carry out cross-border data transfer to maintain business continuity. Even though the Act enables cross-border transfers of personal data with governmental notification, ambiguity about conditions and restrictions might act as a deterrent for multinational companies.[15]

The use of delegated legislation in the Act can also prove to be a challenge. Certain crucial elements of compliance relate to procedural matters and the extent of enforcement. These are intended to be clarified through future rules and notifications. Currently, without the promulgation of the delegated legislation, businesses are required to function in a framework where certain elements of compliance would remain unqualified.[16]

Finally, the matter of organisational compliance is a crucial consideration. For effective compliance with the Act, corporations need to inculcate a compliance culture in themselves. Additionally, training of employees is also a significant imperative. However, it has been noticed that a majority of corporations in India do not have the capabilities to implement them in an efficient manner.

---

[14] Anushka Jain and Prateek Waghre, 'IFF's first read of the draft Digital Personal Data Protection Bill, 2023' (*Internet Freedom Foundation*, 03 August 2023) <https://internetfreedom.in/iffs-first-read-of-the-draft-digital-personal-data-protection-bill-2023/> accessed 01 March 2026

[15] Digital Personal Data Protection Act 2023, s 16

[16] *Ibid* s 40

These factors tend to indicate that although the Digital Personal Data Protection Act, 2023, has a solid compliance framework, it faces tough times during its execution in Indian corporations. It is a pertinent requirement to deal with all such hurdles so that data protection law becomes a facilitator for good corporate governance and not a hindrance to it.

ENFORCEMENT AND ACCOUNTABILITY MECHANISM

The efficiency of any regulatory regime not only lies in fulfilling duties that it imposes, but it also depends upon its enforcement power, clarity, and fairness. The Digital Personal Data Protection Act, 2023, introduces an ample and robust enforcement structure through its Data Protection Board of India.[17] This is a complete shift from its previous enforcement regime under the Information Technology Act, 2000, wherein it solely leaned upon piecemeal approaches.

The Data Protection Board is given the authority to investigate complaints, identify cases involving non-compliance, and administer fines as a result of contraventions to the Act.[18] The fines levied as a result of contraventions to the Act are rather severe, with severe financial implications for contraventions involving fundamental responsibilities such as preventing unauthorised data breaches, as well as failing to comply with fiduciary responsibilities. From a corporation's perspective, this enforcement mechanism also presents new risks associated with compliance as part of its fundamental responsibilities related to its governance structure.

However, arising from these provisions are some doubts as to the extent of discretion exercised by the enforcement authority. Indeed, very little guidance has been issued by the Act as to the issues that need to be taken into consideration in arriving at the amount of the fine. While a good degree of discretion might lead to a quick- response mechanism for enforcement, too much discretion might lead to a lack of predictability for companies as they determine their exposure to enforcement.

Another aspect is the issue pertaining to safeguards on procedures, in view of the fact that, although the Act provides for an adjudication procedure, the absence of stringent procedural guidelines casts a shadow on the matter of consistency, objectivity, and the issue of due process.

[17] Digital Personal Data Protection Act 2023, s 18
[18] *Ibid* s 20

For the corporation, the absence of well-defined procedures for enforcement could hamper interaction with the regulatory body, thereby fueling the fear of arbitrary judicial supervision.

Moreover, the framework of accountability in the Act attempts to ensure deterrence through the threat of high fines, in contrast to the approach of progressive compliance.[19] It needs to be acknowledged that deterrence remains an integral tool for the effectiveness of data protection. However, in the case of innovations in the field of data privacy and small-scale business operations, the presence of a severely punitive policy tool may act as a hindrance.

In summary, the enforcement and accountability regime established under the Digital Personal Data Protection Act, 2023, indicates a clear and strong regulatory posture for enforcement. Yet, the degree to which this regime will prove to be effective would necessarily depend on the manner in which enforcement discretion is exercised.[20] This would undoubtedly prove to be a challenge for Indian corporations, thereby supporting the need for development.

COMPARATIVE INSIGHT

A brief comparative study would enable an understanding of the position that India's data protection framework occupies within the international framework and identify the highlighted features of the Digital Personal Data Protection Act, 2023. Most countries have adopted an overarching framework to govern data protection, which requires corporations to adhere to it, while also paying importance to proportionality and legal certainty.

The General Data Protection Regulation of the European Union is a globally prominent example of a data protection framework.[21] The GDPR has a rights-heavy focus combined with a heavy emphasis on compliance. The GDPR has a focus on consent combined with a right to data minimisation. The GDPR has a strong focus on accountability. A key characteristic of the GDPR is that it prefers specific regulatory guidelines. The Indian framework has a greater focus on principle-based legal obligations. In turn, this makes the Indian framework more flexible. However, for corporations, such a framework means there is a lack of certainty.[22]

[19] Digital Personal Data Protection Act 2023, s 33
[20] *Ibid* ss 27-30
[21] General Data Protection Regulation 2016
[22] *Ibid* art 6

Similarly, countries like the United Kingdom and Singapore have also developed models of data protection that entail both enforcement and advisory measures. The regulatory bodies in such countries are actively involved in issuing codes and guidelines that support corporate compliance. This is an indication that their philosophy of regulation is based on encouraging corporate compliance.[23]

In comparison with these approaches, the Indian approach of prioritising deterrence through penalisation, with little guidance on compliance standards in data protection legislation, shows greater concern for the gravity of data protection compliance. However, the approach also presents concerns in relation to proportionality and the ease of implementation of the law, especially in the case of small and medium-sized businesses. It can thus be observed from the comparative approach that the implementation of data protection legislation also needs compliance assistance mechanisms.

SUGGESTIONS AND WAY FORWARD

In order to make the Digital Personal Data Protection Act, 2023, a successful regulatory measure for corporations in India, there are several steps that need to be taken into consideration to counter the challenges of compliance. The effectiveness of the Act will require more than the absence of punishment for violations.

To begin with, there is a need for greater clarity in regulations. The formulation of rules and guidelines on compliance will aid in this effort. Corporations will then be able to decipher how these have to be followed. There should be clarity in matters related to consent, security, and breach of security.

Secondly, there is a need to create a system of proportional compliance, especially in relation to small to medium enterprises. Tailored obligations depending on the size and level of risk involved in processing activities are essential in ensuring that smaller enterprises are under no obligation to mount disproportionate burdens. What is important is encouraging innovation while still having high levels of protection.[24]

---

[23] UK Data Protection Act 2018; Personal Data Protection Act 2012 (Singapore)
[24] 'Privacy and data protection' (*OECD*) <https://www.oecd.org/en/topics/privacy-and-data-protection.html?__cf_chl_tk=owGO7F_lLbJsPwe.k.gtbM4eRddjeur0gJHhlK18fUs-1775206182-1.0.1.1-eutdngdNZ.PutQN1PbqorpIKX.LT8Pfm8R45FuAGccQ> accessed 01 March 2026

Third, it is recommended that a well-targeted strategy of enforcement should combine elements of deterrence, correction, and advice. Though punishment is a crucial tool in inducing compliance, a regulatory engagement strategy of warnings, compliance directions, and capacity-building measures might just bring about voluntary compliance. The Data Protection Board has a constructive function to play in making interpretative guidelines.[25]

Fourth, capacity building for businesses must be given due importance. Companies must be encouraged to embed data protection as part of their internal governance structure through employee training and accountability. Trade and professional bodies can help create standardised instruments for companies to become compliant.[26]

At long last, periodic legislative review of the Act will enable it to remain responsive to technological and economic development. Periodic review will enable assessments of outcomes of compliance as well as feedback from stakeholders. This will enable the data protection law to keep up with reality.

CONCLUSION

The Digital Personal Data Protection Act, 2023, is a major landmark in India's movement towards establishing a holistic regime of data governance.[27] Though making corporations liable through a statutory mandate and having a unified body to ensure compliance, it is intended to ensure the privacy rights of individuals are better safeguarded, without making corporate practices of utilising data in business unregulated.

In conclusion, the above discussion has analysed the challenges of compliance for Indian corporates as per the provisions of the Act. The law indicates a robust regulatory thrust. However, the lack of detailed guidance provisions, resort to delegated legislation, as well as costly provisions related to compliance, may constitute barriers to the successful implementation of the law, especially for smaller companies.

[25] Digital Personal Data Protection Act 2023, ss 18-20
[26] General Data Protection Regulation 2016, arts 24 and 32
[27] Digital Personal Data Protection Act 2023

The findings of this study are that the rules of data protection in India should maintain a delicate balance between regulatory accountability and ease of business.[28] It is a fact that a regulatory style of compliance and intervention is likely to yield effective and long-term results regarding data governance. With supportive regulatory intervention and engagement, the Digital Personal Data Protection Bill of 2023 will not only be a punitive act for corporates. It will also help to ensure good corporate conduct.

The success of the Digital Personal Data Protection Act, 2023, will be largely determined by how the regulatory authorities determine how to enforce and interpret the Act's provisions.[29] Corporations must be able to comply with the Act via both regulations and penalties; both of these will help ensure compliance with the Act.[30] Therefore, the regulatory framework must be proportional and balanced to ensure that the burden placed on corporations by having to comply with these obligations does not stifle innovation, investment or ease of doing business. The Act, if interpreted and clarified so that there is consistent enforcement, has the potential to create robust and globally aligned data protection issues as India becomes a data-driven digital economy.

[28] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1
[29] Digital Personal Data Protection Act 2023, ss 18-20
[30] *Ibid* s 33