The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2026
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DATA PROTECTION COMPLIANCE IN INDIAN CORPORATES: CHALLENGES AND SOLUTIONS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Palak Anand

INTRODUCTION

Digital Economy in India is a changed landscape of how companies in India maintain and manage personal data. There are digital payments and services, AI, and e-commerce. There are large-scale data processing as core business strategy. However, there are monopolistic business expansion, individual privacy, data misuse, and the absence of accountability. 2023 Digital Personal Data Protection Act is the first in India as a data governance legislation to provide a framework to balance organization accountability with safeguarding data principal rights and the wrongful processing digital personal data.[1] Core principles of the Act are processing data lawfully, purpose specification, consent, grievance mechanism, data breach notification and related penalties, while being a business rationale are compliance, loss to a breach, regulatory fines.[2] There are more than 50 challenges restatement the promise of the DPDP Act to corporates in India, especially limited infrastructure, internal data mapping, third party system, regulatory compliance, and data security.[3] Other challenges to less compliance budget and technical resources which are more by micro and small registered businesses.

The Act requires businesses to fundamentally change how they think of data as an asset because of their focus on consent, data minimization, and how they allocate data purpose. Businesses must shift from broad and open-ended collection data regimes to rights-based, and privacy-centric models. These challenges, it becomes extremely important to seek profitably viable

[1] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[2] Ibid (1)
[3] NASSCOM, *SME Digital Transformation Report* (2023).

ways for Indian corporations to comply with the DPDP.[4] Internal policy changes, employee awareness training, automated tools for consent management, privacy compliant-by-design models, and continuous internal audit mechanisms may offer reasonable means to compliance.[5] Indian businesses must be made aware of these compliance challenges to be responsible for the gaps in consumer trust, and in the absence of consumer confidence, the lack alignment of the Indian economy with international standards for data privacy will be even more pronounced.

OVERVIEW OF THE DPDP ACT, 2023

The Digital Personal Data Protection Act 2023 (DPDP Act) is India's first focused data protection legislation which seeks to protect digital personal data and bolster privacy on an individual level. This legislation targets data protection in India for the first time and comes in the wake of the Supreme Court's declaration of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India. The Act lays down a first of its kind comprehensive regime on the collection, processing, storage, and transfer of personal data.[6] The Act is applicable to all digital personal data processed in India. The Act also applies to processing outside India which is linked to the provision of goods or services to persons in India.[7] The Act is also based on principles of lawful purpose, informed consent, data minimization, and storage limitation. Consent is to be specific, informed, and able to be withdrawn at any time. This is to ensure transparency in data practices.[8] The Act also refers to "legitimate uses" of the data, within which data may be processed without need for express consent, for instance, state functions and emergencies.[9] In a bid to fortify user rights, the DPDP Act also entails the rights of individuals regarding information to access, correct, erase, and amplify grievance redress mechanisms. Data fiduciaries, in particular, Significant Data Fiduciaries, are expected to comply with enhanced responsibilities such as appointing Data Protection Officers and performing impact assessments.[10] Enforcement of this provision rests with the Data Protection Board of India, which has the authority to conduct inquiries concerning violations and to impose significant fines.[11]

[4] Graham Greenleaf, India's Data Protection Developments, 174 Privacy Laws & Bus. Int'l Rep. 1 (2023).
[5] PwC India, *Data Governance & Privacy Frameworks for Indian Enterprises* (2024).
[6] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[7] Digital Personal Data Protection Act, No. 22 of 2023, S. 3 (India).
[8] Ibid 7 (S.4-7)
[9] Ibid S.6
[10] Ibid S.7
[11] Ibid S.11-13

KEY CHALLENGES FOR INDIAN CORPORATES

The introduction of the Digital Personal Data Protection Act, 2023 (DPDP Act) brings a very broad scope of compliance, operation, and organisational challenges to the Indian corporates. The transition to a consent-driven data governance model, requiring specific, informed, and granular consent of Data Principals, is one of the most significant challenges, and may need to be redesigned to guarantee the implementation of all necessary requirements.[12] The transition to a consent-based data governance model, where there is a required specific, informed, and granular consent of Data Principals, has become one of the most important issues, and it may require redesigning websites, mobile apps, and customer-onboarding systems.[13]

Working on data minimisation, purpose limitation and storage limitation is also experienced by corporates with significant challenges, so e-commerce, fintech, insurance and ed-tech industries will need to reassess their data-retention policies and reduce superfluous data collection. One of the significant challenges is the requirement to have reasonable security controls and implement effective breach-notification systems.[14] A large number of businesses do not have established security systems and need to spend much money on the technological improvements and 24/7 surveillance. Such upgrades have massive financial and human-resource costs, especially to MSMEs.

There are also Significant Data Fiduciaries (SDFs) with increased compliance burdens such as compulsory Data Protection Impact Assessment (DPIA), Data Protection Officer (DPO) appointment and regular audits, which can be hard to hire or costly. Another emerging barrier is compliance of cross-border data-transfer.[15] Companies that are involved in international business or dealing with the foreign suppliers will need to re-evaluate contracts, guarantee legal transfer processes and update the internal data-transfer policies according to the lists notified by the government. At the organisation level, organisations face lack of awareness among the employees, reluctance towards updated protocols and necessity of massive capacity-building programmes. These issues combined point to the fact that DPDP compliance is not simply a formal procedure, but an overall revision of corporate data governance ecosystems.

PROPOSED SOLUTIONS FOR EFFECTIVE COMPLIANCE

[12] Ibid S.8
[13] Ibid S.10
[14] Ibid S.19-33
[15] Ministry of Electronics & Info. Tech., *DPDP Compliance Advisory* (2024).

Indian companies would need a multi-layered compliance system in order to cope with the complexities of the Digital Personal Data Protection Act, 2023 (DPDP Act) and guarantee a smooth implementation of the compliance process. The initial requirement is the installation of a solid system of consent management. Organisation should re-architecture user interfaces in order to display easy to understand consent notices and offer easy to understand, transparent mechanisms to withdraw consent.[16] Implementing automated consent-tracking programs can minimise mistakes and enhance audit readiness.

Corporates also need to create and implement extensive internal data-governance policy. This involves data flow mapping, purpose of process identification, retention schedule, and role-based restrictions.[17] Frequent internal audits are a means of ensuring that there is a constant application of the principles of data minimisation, limitation of purpose, and limitation of storage. Cybersecurity infrastructure is another important step to take. Incorporating industry-standard encryption strategies, intrusion-detection systems, and endpoint security strategies allow businesses to satisfy the reasonable-security safeguard requirements in Section 8.[18] Establishing an incident response team and breach-notification procedures will allow businesses to communicate with the Data Protection Board in a timely manner in the event of the data breach.

In the case of companies that are Significant Data Fiduciaries (SDFs), without exception, the compliance should include the appointment of experienced Data Protection Officers (DPOs), Data Protection Impact Assessment (DPIA), and processing documentation. These are applicable measures to mitigate privacy risks at an enterprise level.

Corporates involved in cross-border processing are supposed to develop standardised data-transfer contracts, screen foreign suppliers on compliance preparedness, and implement government-accepted transfer systems on being informed. Another long-term solution is the creation of an organisational culture that is responsive to privacy. Frequent training programme, staff sensitisation training sessions and through regular compliance reminders can reduce internal violations and hold institutions to account.

Finally, policy enforcement could be made easier through the adoption of RegTech and AI-oriented compliance tools, which will help to automatize the gap assessment and offer real-

[16] Supra (1)
[17] Ibid S. 8(5)
[18] Ibid (15)

time data about privacy risks.[19] All these solutions are aimed at assisting corporates to overcome careful compliance to active privacy governance so that business practices align with international standards.

IMPACT OF DPDP COMPLIANCE ON CORPORATE STRATEGY

The Digital Personal Data Protection Act, 2023 (DPDP Act) is transforming the strategic priorities of the Indian corporates, which require them to make privacy and data protection central to the business decision-making process. Compliance is no longer a legal obligation practiced at the back-end of many organisations but a strategic driver that has altered growth models, technological investments and trust amongst the stakeholders.[20]

The greatest effect is the move towards privacy-by-design, which means that businesses must design data protection into their products, platforms, and workflow processes at the very beginning. Firms are forced to devise interfaces exceeding user interfaces in emphasis on transparency, granular consent, and minimal data collection, and have fundamentally changed the models of customer-engagement.

The risk management and governance framework are also affected by compliance requirements. The re-organization of internal controls, the creation of data committees, and the implementation of enterprise wide data-governance systems is what will reflect the move towards an all-embracing risk mitigation with regard to statutory requirements under Sections 4-10 of the Act.[21]

Regarding market positioning, high DPDP adherence would supercharge brand credibility and consumer trust which will give corporates a competitive advantage in data-sensitive industries (such as fintech, e-commerce, and health-tech) through strategic decision-making in product launches, expansion, and partnerships with third parties , and non-compliance would lead to devastating financial fines, operational consequences, and brand reputations, affecting strategic decision-making.[22] The other significant effect is the increase in emphasis on modernisation of technology. To ensure that businesses comply with statutory requirements, corporates are putting more money in secure cloud infrastructure, encryption technologies, and automated compliance tools.

---

[19] Ibid (13)
[20] Digital Personal Data Protection Act, No. 22 of 2023, § 8(3) (India).
[21] Deloitte, *Privacy Maturity and Consumer Trust Report* (2024).
[22] Digital Personal Data Protection Act, No. 22 of 2023, §§ 19–33.

Lastly, compliance with DPDP affects the business strategies of the world. Cross-border companies are required to match the global privacy standards, reconsidering the vendor contracts as well as the data-transfer systems. [23] This harmonisation opens up the way to the seamless global operations and scalability in the future. All in all, DPDP compliance is an engine of strategic change and not a form of imposed obligation.

CONCLUSION

The adoption of the Digital Personal Data Protection Act, 2023 (DPDP Act) is a landmark event in the history of regulatory development in India and a sign of a new wave into the rights-oriented and accountable data ecosystem. The Act radically transforms the current state of privacy practices by making corporates collect, store, and use personal data through a systematic set of obligations, an obligation that concerns consent, lawfulness, data minimalization , data transparency, and data security assurances. Even though the implementation of the DPDP Act is associated with significant structural, financial, and technological costs, particularly to the industries with large volumes of data, the dividends of a vigorous privacy stance significantly outmatch the upfront costs. Successful compliance will promote consumer trust, brand recognition, and align business operations with international privacy standards like the GDPR. This alignment is especially vital to the business companies that operate internationally, those that engage in technology alliances, or those that expand their markets.

In addition, the Act also promotes privacy-by-design, risk-based data management, and cyber-resilience, which consequently mitigates exposure to breach, regulatory fines, and reputation loss. Additional measures like the creation of specialised posts like Data Protection Officers and the necessity of Data Protection Impact Assessments of Significant Data Fiduciaries only ensure that privacy is a proactive organisational principle and not a responsive compliance effort. Finally, the DPDP Act cannot be perceived as a problematic regulation rule but rather as a driver of the digital transformation. Investing in safe and sound infrastructure, open data-management systems, and effective internal accountability systems can help corporates attain compliance besides improving operations and competitive edge. With a fast-paced digitalising economy, organisations that are more concerned with the security of their data will find it easier

[23] Ibid (17)

to innovate in a responsible way, protect the trust of their users, and succeed in the emerging global digital environment.

REFERENCES

1. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
2. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
3. Ministry of Electronics & Information Technology, DPDP Compliance Advisory (2024).
4. Deloitte, Privacy Maturity and Consumer Trust Report (2024).
5. Central Government (India), Press Information Bureau Release on DPDP Act Implementation (2023).
6. NASSCOM, Data Protection Readiness Survey: Industry Insights Post-DPDP Act (2024).
7. Rishabh Dara, *Data Protection in India: The Road to Reform*, 12(3) NLSIR 45 (2023).
8. Aparna Vishwanathan, *Understanding India's Data Governance Framework*, 18 Indian J. L. & Tech. 120 (2024).
9. Ananth Padmanabhan, *Privacy Law in India: Emerging Trends Post-DPDP Act*, 42 Nat'l L. Sch. India Rev. 233 (2024).
10. Rahul Matthan, The Future of Data Protection in India (2024).