DHARANA
International Journal of Business

https://doi.org/10.18311/DBIJB/2025/53046

Stakeholder Theory and the Reconfiguration of Power, Responsibility, and Compliance under India's DPDP Act 2023

S. Vijayalakshmi

Abstract

The Digital Privacy Protection Act 2023 reshapes the ethical and management frameworks encompassing digital privacy in India. The Digital Privacy Protection Act 2023 reshapes the ethical and management frameworks encompassing digital privacy in India. Based on Freeman, Stakeholders Theory, this paper examines how digital legislation reconfigures institutional power, responsibility and compliance and creates value by redefining the relationship between employers (data fiduciaries), employees (data subjects) and regulators, as outlined in DPDP Act 2023. Consent and responsibility-based techniques will engage employees as active partners, thereby increasing trust and transparency in the institution. Incorporating stakeholders' perspectives enhances ethical liability as a driving force of legitimacy and competitiveness. As a result, privacy is evolving beyond compliance-based on trust and strategic factors for value creation. This paper highlights the significance of stakeholders in promoting ethical governance, trust and institutional resilience in today's digital economy.

Keywords: Data Privacy, DPDP Act 2023, Compliance, Power, Responsibility, Stakeholders' Theory

JEL Classification: D63, K24, M14

Cite this article as: Vijayalakshmi, S. (2025). Stakeholder Theory and the Reconfiguration of Power, Responsibility, and Compliance under India's DPDP Act 2023. *DHARANA - International Journal of Business, 16*(2), 79–85. doi: https://doi.org/10.18311/DBIJB/2025/53046

Introduction

A right to privacy is explicitly stated under Article 12 of the 1948 Universal Declaration of Human Rights: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (United Nations Assembly, 1948, p.6).

S. Vijayalakshmi

Assistant Professor, M P Birla Institute of Management, Bengaluru – 560001, Karnataka, India; lamysster@gmail.com; ORCID ID: https://orcid.org/0009-0003-6245-1085

Privacy is both an individual and an organisational concern; if the information is misused, it leads to serious consequences for the firm. On the contrary, when personal information is utilised ethically, it safeguards the firm and also becomes one of the sources of competitive advantage. Moreover, ethical information practices are crucial for supporting every activity across the organisational value chain. (Culnan & Armstrong, 1999). The Digital Personal Data Protection Act 2023, popularly known as the DPDP Act, is India's data privacy legislation. (Ministry of Electronics and Information Technology (Government of India, 2023). It establishes a legal framework for the processing of digital personal data. (Safna, 2025; Tandon & Gupta, 2025). The DPDP Act mandates responsible data handling, grants individuals increased control over their personal data, and accountability for Data Fiduciaries (DFs) (Press Bureau Information, 2023). The increasing predominance of data privacy law across the world has reframed how firms govern employee data, with the European Union's GDPR serving as a global point of reference. (Voigt & von dem Bussche, 2017). DPDP Act 2023 introduces digital personal data, consent, data minimisation, data processing and accountability at the core of employee personal information management within the organisation. (Saha & Mukhopadhyay, 2024). The Data Protection Directive expands employees' rights as data subjects, imposes new fiduciary obligations on employers, transparency regulations, security guarantees and a grievance redress framework. (RegTech Times, 2023). However, these shifts give rise to organisational and regulatory challenges. Employers are urged by labour, tax, and compliance laws to collect and store sensitive data, which may cause friction with the Act's consent-based framework (Saurabh, 2024). These aspects create uncertainty in implementation and concerns about compliance liability, data governance and trust at the workplace. This paper aims to critically explore how stakeholder theory can reform or transform the dynamics of power between institutions and individuals, the allocation of responsibility in data management, compliance behaviour under new legal mandates, and the promotion of inclusive accountability.

DPDP Act 2023 and GDPR

General Data Protection Regulation (GDPR) is regarded as the world's strongest data protection regulation and acts as a perfect guiding principle for all countries. In the historic ruling of Justice K. S. Puttaswamy (Retd) and Anr vs Union of India 2017, the goal of having dedicated privacy legislation in India was established (Mukhija & Jaiswal, 2023). The DPDP legislation makes major changes to the employee personal data processing of companies in India and those outside India providing goods and services to people in India. The DPDP Act 2023 mandates organisations' data handling, grants individuals control over their personal data, and enforces accountability for DFs. Furthermore, the DPDP Act is designed to safeguard the rights of Data Principals (DPs) regarding personal information (Latham & Watkins, 2023). In contemporary privacy legislation, the data minimisation principle is pivotal. These aspects position the DPDP Act 2023 to advance and align with global standards in privacy protection, such as those established by the GDPR. (Bharanitharan & Kaur, 2024). The positive outcome of the DPDP Act 2023 is that companies not only store employee data in India but also allow cross-border data flows. (Gupta & George, 2025).

The Stakeholder Theory

Stakeholder theory (Freeman, 1984) provides a multi-faceted model for understanding how regulatory pressure, organisational culture, data protection, and accountability frameworks interact to influence trust, perceived legitimacy and compliance within the organisations. In Stakeholder theory, Freeman posits that organisations must consider the interests of all stakeholders, and not just shareholders. This includes employees, customers, government, regulators and the community at large. Valentinov and Roth (2024) postulate that the stakeholders create reciprocal relationships which require ethical convergence and transparency. The DPDP legislation institutionalises this logic by mandating consent-based data management, fiduciary responsibility and grievance mechanisms, thus embedding ethical accountability in corporate governance.

Conceptual Framework

Previous literature research papers examine consumer-centric impacts of data privacy (Bennett, 2018; Tikkinen-Piri *et al.*, 2018), largely focusing on customer-centric aspects. Indian DPDP Act 2023 represents a structural shift from a traditional, informal, employer-centric to a consent-driven, accountability-based framework. The stakeholder Theory conceptualises an organisation as an intricate linkage, where reciprocal and changeable interactions with stakeholders determine actual operational legitimacy and performance. Government regulators play a vital role in shaping how organisations handle data, requiring them to follow rules and helping set cultural standards. Building a strong culture of data protection within a company promotes ethical handling of employee information and creates an environment of trust and safety. When employees understand how their data is used and protected, they become more engaged and are better able to support and take part in responsible data practices. (Valentinov & Roth, 2024).

Redefining the Responsibility in the Context of DPDP

Before the enactment of the Digital Personal Data Protection Act, organisational responsibility in data management was largely confined to basic legal compliance requirements. The DPDP Act 2023 establishes a framework of shared ethical responsibility among stakeholders, in line with the principles of stakeholder theory. (Harrison *et al.*, 2010). *Employers (Data Fiduciaries)*: Must collect and process employee data lawfully, purposefully, and securely. *Employees (Data Principals)*: Gain the right to consent, access, correction, and grievance redressal. *Regulators*: Act as oversight bodies to ensure procedural fairness and accountability (Government of India, 2023, p. 2).

This triadic responsibility distribution reflects Freeman's (1984) stakeholder perspective, where companies earn credibility and trust of all affected parties through ethical and fair treatment. Ethical information handling thus becomes both a compliance requirement and a strategic capability enhancing trust, loyalty, and organisational resilience (Mitchell *et al.*, 1997).

From Data Controlling to Employee Data Collaboration

The DPDP Act reshapes conventional corporate data management by shifting the balance of

power, giving individuals greater control over their personal data and promoting shared data rights (Zuboff, 2019). Through consent-based processing, employees are positioned as active participants rather than passive subjects of data. They have enforceable rights that force organisations to justify any action with data. This decentralisation of data power creates a culture of data partnership in which employers, employees, and regulators work together to maintain digital trust. Power no longer derives solely from data possession, but also from ethical management and transparent procedures. This is consistent with Freeman's proposal that sustainable corporate power derives from the legitimacy of the stakeholders rather than from dominance or control (Parmar *et al.*, 2010).

Value Creation, Ethical and Competitive Advantage

From the perspective of stakeholders, the creation of value goes beyond economic metrics and includes ethical legitimacy, transparency and trust (Parmar *et al.*, 2010). The Data Protection Directive provides the basis for building corporate digital responsibility, which integrates privacy, integrity and sustainability into corporate digital strategies, by making compliance a competitive asset rather than a constraint, and by building trust and confidence in the process (Kramer & Porter, 2011).

Engaging and Balancing Stakeholders

The effective implementation of the Data Protection Directive requires a structured stakeholder engagement strategy, including identification, communication and balancing of different interests (Clarkson, 1995). This may further be explained as: (i) *Identification*: Mapping of internal and external stakeholders affected by data policies (employees, regulators, vendors and consumers); (ii) *Communication*: Promoting awareness through consent platforms and transparent communication, and (iii) *Balancing*: the data rights and operational efficiency, harmonising the corporate value chain.

Ethical, Inclusive and Sustainable Outcomes

In the context of data protection, stakeholder theory reflects a form of digital citizenship, encouraging shared responsibility among individuals and institutions to uphold fairness, transparency, and protection for data privacy. (Florida *et al.*, 2018). The effectiveness of the DPDP Act hinges on closing enforcement gaps and raising public awareness. (Kadari & Valaboju, 2025).

Integrative Conceptual Stakeholder Framework

This Conceptual framework depicts how the DPDPD Act 2023 reshapes the interactions of power, responsibility, and compliance among stakeholders. Variables are explained as:

(i) *Stakeholders Group*: Includes the het participants in the data ecosystem, such as employees, employers, organisations, third-party vendors, regulators, and society at large, who play a vital role in data governance.

(ii) *DPDP Role/Obligation*: Defines rights, responsibilities, and functions allocated to each stakeholder under the DPDP Act 20233.

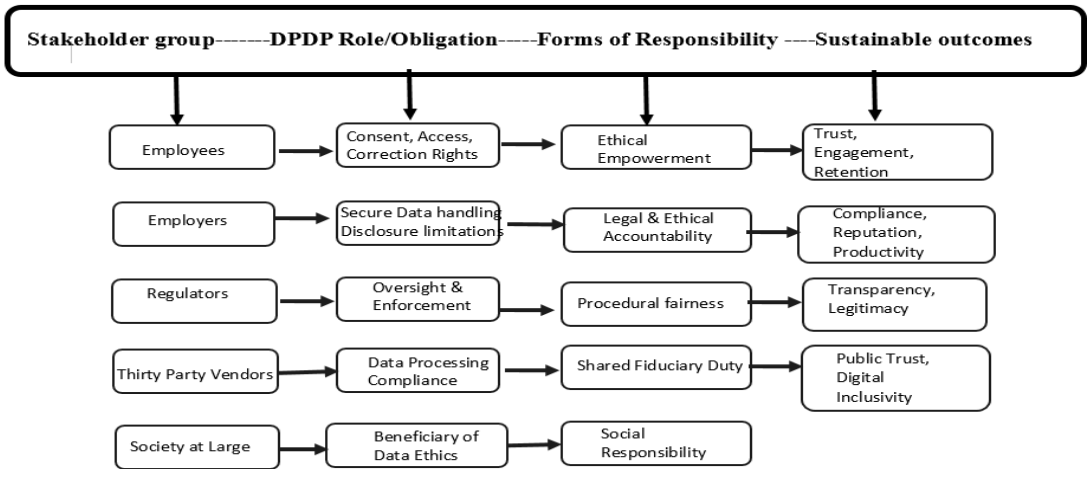


Figure 1. Integrative Conceptual Stakeholder Framework
Source: Based on Compilation of the Author's Work

(iii) *Forms of Responsibility*: represent legal obligations, operational commitment, and accountability in data practices.

(iv) *Sustainable Outcomes*: highlights the outcomes, such as trust and innovation that arise when stakeholders fulfil their responsibility. This structure connects the roles of employees, employers, vendors, and society, built on an ethical and transparent data ecosystem. By synchronising legal obligations with moral accountability, the Act transforms compliance from a legal requirement to an ethical responsibility. This promotes trust, transparency, and digital inclusivity, ultimately reconfiguring governance into to participatory and trustworthy digital environment.

Conclusion and Future Research Directions

The Digital Privacy and Data Protection Bill, 2023, marks a significant shift in how corporate responsibility and data governance are approached in India. By integrating stakeholder theory, this paper argues that ethical compliance, inclusivity and sustainability form the foundation for public trust and credibility in today's digital world. The DPDP legislation turns privacy into legal compliance, which is a cornerstone of corporate digital responsibility. However, a major challenge lies in the enforcement capacity of the Data Protection Board (DPB), which remains uncertain due to limited resources and India's huge digital ecosystem (Chander, 2024). Further empirical research should examine this connection using quantitative research methods like structural equation modelling or partial linear regression, to better analyse how stakeholder involvement contributes to building trust, compliance, and enriching corporate reputation in future. In addition, cross-sectorial peer review research can reveal how stakeholder-inclusive approaches to data protection contribute to ethical resilience as well as economic benefit.

References

Bharanitharan, K., & Kaur, G. (2024). A comparative analysis of data minimisation principles: Evaluating GDPR and India's DPDP Act 2023. *International Conference on Data Mining and Information Security* (pp. 41-55). Springer Nature, Singapore. https://doi.org/10.1007/978-981-96-6046-9_3

Bennett, C. J. (2018). The European General Data Protection Regulation: An instrument for the globalization of privacy standards? *Information Polity, 23*(2), 239–246. https://doi.org/10.3233/ip-180002

Chander, A. (2024). Data protection in India: The need for a robust framework. *Journal of the Indian Law Institute*, *56*, 123.

Clarkson, M. B. E. (1995). A stakeholder framework for analyzing and evaluating corporate social performance. *Academy of Management Review, 20*(1), 92. https://doi.org/10.2307/258888

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104-115.

Florida, R., Adler, P., & Mellander, C. (2018). The city as innovation machine. *Transitions in regional economic development* (pp. 151-170). Routledge. https://doi.org/10.4324/9781315143736-8

Freeman, R. E. (1984). *Strategic management: A stakeholder approach*. Pitman, Boston, MA.

Government of India. (2023). *Digital Personal Data Protection Act, 2023 (Act 22 of 2023)*. Ministry of Law and Justice. https://indiankanoon.org/doc/3510545/

Government of India. (2023). *Digital Personal Data Protection Act, 2023*. Gazette of India. https://www.meity.gov.in

Gupta, N., & George, A. (2025). Digital Personal Data Protection Act, 2023: Charting the future of India's data regulation. *Data governance and the digital economy in Asia* (pp. 34-53). Routledge. https://doi.org/10.4324/9781003505723-3

Harrison, J. S., Bosse, D. A., & Phillips, R. A. (2010). Managing for stakeholders, stakeholder utility functions, and competitive advantage. *Strategic Management Journal*, *31*(1), 58-74. https://doi.org/10.1002/smj.801

Kadari, R., & Valaboju, P. (2025). Clouds of reason: An empirical study of governance, privacy, and predictive intelligence. *International Journal of Recent Contributions from Advanced Information Technology*, *8*(3), 9-25. https://doi.org/10.34218/IJRCAIT_08_03_002

Kramer, M. R., & Porter, M. (2011). *Creating shared value* (Vol. 17). Boston, MA.

Latham & Watkins (2023). India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison. *In India's Digital Personal Data Protection Act 2023 Vs. The GDPR: A Comparison.*

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. *Academy of Management Review*, 22(4), 853-886. https://doi.org/10.5465/amr.1997.9711022105

Mukhija, K., & Jaiswal, S. (2023). Digital Personal Data Protection Act 2023, in light of the European Union's GDPR. *Jus Corpus Law Journal*, *4*, 638.

Parmar, B. L., Freeman, R. E., Harrison, J. S., Wicks, A. C., Purnell, L., & De Colle, S. (2010). Stakeholder theory: The state of the art. *Academy of Management Annals*, *4*(1), 403-445. https://doi.org/10.5465/19416520.2010.495581

Press Information Bureau. (2023, August 11). The Digital Personal Data Protection Act, 2023 [Press release]. https://www.pib.gov.in

RegTech Times. (2023). *India's digital data protection regulation*. https://regtechtimes.com/indias-digital-data-protection-regulation/

Safna. (2025, June 28). Cookie Consent Trends by Country: 2025 Global Compliance Guide. *CookieYes*. https://www.cookieyes.com/blog/cookie-consent-trends/

Saha, S., & Mukhopadhyay, S. (2024). A new age of data privacy laws in India: Review of Digital Personal Data Protection Act, 2023. *Indian Journal of Legal Studies*, *10*, 84-95.

https://doi.org/10.60143/ijls.v10.i1.2024.114

Saurabh, S. (2024). The Digital Personal Data Protection Act of 2023: Strengthening privacy in the digital age. *International Journal of Law in Changing World*, *3*, 77. https://doi.org/10.54934/ijlcw.v3i2.84

Tandon, U., & Gupta, N. K. (2025). Informational Privacy in the age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023. Legal *Issues in the Digital Age, 6*(2), 87–117. https://doi.org/10.17323/2713-2749.2025.2.87.117

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

United Nations. (1948). Universal Declaration of Human Rights, United Nations. *UN General Assembly*, *302*(2), 14-25.

Valentinov, V., & Roth, S. (2024). Stakeholder theory: Exploring systems-theoretic and process-philosophic connections. *Systems Research and Behavioral Science*, *41*(2), 301-315. https://doi.org/10.1002/sres.2970

Voigt, P. and Von dem Bussche, A. (2017) The EU General Data Protection Regulation (GDPR): A Practical Guide. 1st Edition, *Springer International Publishing, Cham*. https://doi.org/10.1007/978-3-319-57959-7

Zuboff, S. (2019). Surveillance capitalism and the challenge of collective action. *New Labor Forum*, *28*(1), 10-29. Sage Publications. https://doi.org/10.1177/1095796018819461