2026 Volume: 02 Issue: 11 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-09

CORPORATE GOVERNANCE AND DATA PRIVACY: THE LEGAL RESPONSIBILITY OF INDIAN COMPANIES FOR UNAUTHORISED SHARING OF CUSTOMER DATA

***Khushi Bansal**

India.

Article Received: 02 October 2026
Article Revised: 22 October 2026
Published on: 12 November 2026

***Corresponding Author: Khushi Bansal**
India.

DOI: https://doi-doi.org/101555/ijrpa.9131

ABSTRACT

Customer data is now among the most valuable and most vulnerable assets of an Indian company. This paper examines who bears legal responsibility when that data is shared without authorisation, and under which instruments. It argues that responsibility in India is layered. They do not, however, give affected customers a right to compensation, and they create no individual liability for directors. That task falls to the Companies Act, 2013, the SEBI listing regime, the Information Technology Act, 2000 ("IT Act") and general criminal and consumer law. The paper maps these layers, examines how liability is attributed between company, board, officers and vendors, compares the Indian position with the GDPR and United States oversight doctrine, and proposes reforms. The paper also examines the role of third-party service providers, technology vendors and data processors in handling customer information.A comparative analysis of the European Union's General Data Protection Regulation (GDPR) and relevant developments in United States corporate oversight law is undertaken to identify possible lessons for India. The comparison focuses on regulatory enforcement, compensation for affected individuals, directors' oversight responsibilities and the remedies available to customers.It requires a preventive approach involving stronger board-level supervision, transparent data-handling practices, effective grievance redressal mechanisms and proportionate consequences for corporate and individual misconduct.

KEYWORDS: DPDP Act 2023; Data Fiduciary; corporate governance; directors' duties; personal data breach; Companies Act 2013; SEBI LODR.

I. INTRODUCTION

Every consumer-facing business in India now holds a detailed record of its customers: identity documents, payment credentials, location histories, purchase patterns and, increasingly, health and financial information. This creates two distinct risks. The first is external, where criminals extract the data. The second is internal and more directly a question of governance: the company, its employees or its vendors disclose the data to others without the customer's authorisation, whether through a commercial arrangement, a weakness in the supply chain, or the act of a rogue insider. Widely reported Indian incidents in recent years, affecting online grocery, airline, hospital and health-insurance customers, show that neither risk is hypothetical.[1]

The answer has three dimensions. The first is the company's own liability to regulators and customers. The second is the liability of those who run the company, namely directors, key managerial personnel and other officers. The third is the company's responsibility for the third parties to whom it entrusts data. Indian law answers these questions through statutes that were not drafted together, and the DPDP Act has changed the balance between them. This paper makes three arguments. First, the DPDP Act concentrates accountability in the company as Data Fiduciary and holds it answerable even for the failings of its processors. Second, the Act is silent on individual liability and on compensation, so corporate governance law, in particular directors' duties under section 166 of the Companies Act and the risk-oversight obligations of listed entities, becomes the main route by which responsibility reaches the boardroom. Third, this arrangement leaves gaps that boards should close voluntarily and that policymakers should consider closing by amendment.
The study is doctrinal. It relies on statutes, subordinate legislation, regulatory directions and reported judgments. Several DPDP provisions are not yet in force, and the paper identifies them as it goes.

II. Conceptual Framework

A. What counts as "unauthorised sharing"

In the first, the company itself deliberately discloses customer data to a partner, advertiser or group entity beyond what the customer agreed to. In the second, a vendor or processor to whom the company outsourced a function discloses or loses the data. In the third, an

[1]Pranav Mukul, 'Explained: How big is the BigBasket data breach?', The Indian Express (9 November 2020); Aditya Kalra and Munsif Vengattil, 'Hacker uses Telegram chatbots to leak data of top Indian insurer Star Health', Reuters (20 September 2024). These reports illustrate the range of Indian customer-data incidents; allegations and reported figures should be read with the qualifications stated in the reports.

employee or other insider misappropriates the data and passes it on. In the fourth, an outsider breaches the company's systems. Only the first is truly a sharing decision by the company, but the DPDP Act treats all four alike. The legal analysis therefore turns less on how the data left the company and more on whether the company had a lawful ground for its processing and had taken the safeguards the law requires.

B. Governance theory and the fiduciary idea

Corporate governance in India has traditionally concerned the relationship between management, the board and shareholders.

he Srikrishna Committee then built that regime on the idea that entities which collect data stand in a fiduciary relationship with the individual, and the label "Data Fiduciary" carries the idea into the statute.

This framing matters for governance. That stakeholder-oriented duty makes customer trust a legitimate object of board attention. Agency theory points the same way, since a board that neglects data practices exposes shareholders to regulatory penalty, litigation and reputational loss.

III. The Existing Statutory Framework

A. Section 43A and the SPDI Rules

It makes a body corporate that possesses, deals with or handles sensitive personal data or information in a computer resource that it owns, controls or operates liable to pay compensation where it is negligent in implementing and maintaining reasonable security practices and thereby causes wrongful loss or wrongful gain to any person.[2] The 2011 SPDI Rules supply the detail. They define sensitive data to include passwords, financial information, health conditions, sexual orientation, medical records and biometrics. The regime has well-known weaknesses. It protects only defined categories of sensitive data, it requires proof of negligence and of wrongful loss or gain, and by most accounts its adjudication machinery has been little used.

B. Criminal provisions and the company's officers

It therefore reaches vendors and employees who leak data. Section 85 deals with offences by companies. Every person in charge of, and responsible to the company for, its business is

[2]Information Technology Act, 2000, s 43A (compensation for negligence in implementing and maintaining reasonable security practices where wrongful loss or wrongful gain results).

deemed guilty, subject to proof that the offence occurred without his knowledge or despite due diligence, and a director, manager or officer is also liable where the offence occurred with his consent or connivance or is attributable to his neglect.[3] In Avnish Bajaj v. State (NCT of Delhi), the Delhi High Court held that the managing director of an online marketplace could not be proceeded against for an IT Act offence where the company had not been arraigned as an accused. The Supreme Court later reasoned in the same way in Aneeta Hada v. Godfather Travels and Tours, under the analogous section 141 of the Negotiable Instruments Act, 1881.[4] Prosecutors must therefore build the case around the company first and the individual second.

C. Consumer law and sectoral regulation

The Consumer Protection Act, 2019 lists among unfair trade practices the disclosure to another person of personal information given in confidence by the consumer, unless the disclosure is made under law.[5] A customer whose data was shared without authorisation may therefore complain to a consumer commission for compensation, and the Central Consumer Protection Authority may act against the practice. This route exists independently of the DPDP Act, a point taken up in Part. The DPDP Act and Rules: The Company as Data Fiduciary

A. Status and timeline

The provisions constituting the Data Protection Board of India took effect on notification. The substantive obligations on Data Fiduciaries, including notice, consent, security safeguards and breach notification, are scheduled to apply after eighteen months, around mid-May 2027.[6] Until then, section 43A and the SPDI Rules continue to operate. Boards that wait for 2027 before starting preparation are likely to find the time too short for the data mapping, vendor renegotiation and system changes the Act requires.
B. A company answers for its processorsA "Data Fiduciary" is any person who alone or

[3]Information Technology Act, 2000, s 85 (offences by companies and liability of persons in charge, as well as liability based on consent, connivance or neglect).
[4]Avnish Bajaj v State (NCT of Delhi), 150 (2008) DLT 769 (Del); Aneeta Hada v Godfather Travels and Tours Pvt Ltd, (2012) 5 SCC 661. The latter concerned the analogous rule under s 141 of the Negotiable Instruments Act, 1881.
[5]Consumer Protection Act, 2019, s 2(47)(ix), which includes certain disclosures of personal information supplied in confidence by a consumer within the definition of an unfair trade practice, subject to the statutory qualification.
[6]Digital Personal Data Protection Act, 2023, s 1(2); Ministry of Electronics and Information Technology, notification G.S.R. 843(E), Gazette of India, 13 November 2025 (phased commencement of the Act).

together with others determines the purpose and means of processing personal data, and "person" expressly includes a company.[7] Section 8(1) makes the Data Fiduciary responsible for compliance with the Act in respect of processing undertaken by it or on its behalf by a Data Processor, irrespective of any agreement to the contrary. Section 8(2) permits a processor to be engaged only under a valid contract. The company is therefore the single point of accountability for leaks through vendors, cloud providers, analytics firms and outsourced call centres. It cannot discharge responsibility by contract. It can only manage the risk by selecting, supervising and securing recourse against its processors.

C. Lawful ground for sharing: notice and consent

Sharing customer data with a third party is processing and needs a lawful ground. A request for consent must be accompanied by a notice describing the data, the purpose, and how to withdraw consent and complain, and Rule 3 requires the notice to be clear, itemised and understandable independently of other information.[8] Withdrawal must be as easy as giving consent, and on withdrawal the fiduciary must cease processing and cause its processors to do the same unless the law requires retention. Sharing that exceeds the purposes in the notice, relies on bundled consent It is in this category, the company's own commercial choices, that the DPDP Act has its sharpest effect.These provisions create a governance trigger. A notification to thousands or millions of customers is effectively public, and it forces the board to decide quickly on the facts, the cause and the response. Boards that have not rehearsed this decision against the Companies Act and the listing rules are likely to respond poorly.

E. Significant Data Fiduciaries and the board

Section 10 allows the Central Government to notify a Data Fiduciary as a "Significant Data Fiduciary" having regard to the volume and sensitivity of data, the risk to Data Principals, and the potential impact on India's sovereignty and integrity, electoral democracy, security of the State and public order. Such a fiduciary must appoint a Data Protection Officer based in India who is responsible to the board of directors or similar governing body, appoint an independent data auditor, and undertake periodic data protection impact assessments and audits. Rule 13 adds annual assessment and reporting requirements Because the officer's

[7]Digital Personal Data Protection Act, 2023, s 2(i) (definition of 'Data Fiduciary') and s 2(u) (definition of 'person', which includes a company).
[8]Digital Personal Data Protection Rules, 2025, r 3 (notice requirements), read with Digital Personal Data Protection Act, 2023, ss 5–6 (notice and consent).

reporting line runs to the board, directors cannot later claim ignorance of the company's data risk profile.

F. Penalties, procedure and the compensation gap

Breach Maximum penalty

Failure to take reasonable security safeguards to prevent a personal data breach (s 8(5)) ₹250 crore Breach of any other provision of the Act or Rules ₹50 crore In fixing the amount the Board must consider the nature, gravity and duration of the breach, A Data Fiduciary may offer a voluntary undertaking which, if accepted, bars proceedings on the matter, and appeals against the Board's decisions lie to the Telecom Disputes Settlement and Appellate Tribunal.[9]Three features of this design deserve attention. First, penalties are paid into the Consolidated Fund of India and not to affected customers. Second, section 39 bars civil courts from entertaining suits on matters the Board is empowered to determine, and section 44(2) omits section 43A once it comes into force, so the statutory compensation remedy for customers disappears.[10]. Third, the Act contains no counterpart to section 85 of the IT Act. Penalties fall on the Data Fiduciary, and directors and officers are not mentioned. The Act is expressly in addition to other laws, but prevails over them in a conflict, so individual accountability must come from elsewhere.[11]

V. Corporate Governance: How Responsibility Reaches the Boardroom

A. Directors' duties under the Companies Act, 2013

The company may then proceed against the directors, and members may apply to the National Company Law Tribunal under section 245 for orders restraining unlawful conduct and for damages or compensation from the company or its directors for wrongful acts or omissions.[12]The standard is not strict liability. Indian courts have long held, in the tradition of Official Liquidator v. P.A. Tendolkar, that directors are not answerable for mere errors of

[9]Digital Personal Data Protection Act, 2023, ss 32 (voluntary undertaking), 29 (appeal to the Appellate Tribunal) and 18–26 (Data Protection Board and related provisions).
[10]Digital Personal Data Protection Act, 2023, ss 39 and 44(2). Section 44(2) provides for omission of s 43A of the Information Technology Act when that amendment comes into force; the commencement notification phases this provision in after eighteen months from 13 November 2025.
[11]Digital Personal Data Protection Act, 2023, s 38 (Act to be in addition to and not in derogation of other laws, subject to the statutory rule for inconsistency).
[12]Companies Act, 2013, s 245 (class action proceedings by members or depositors, subject to the statutory requirements and thresholds).

business judgment but only for misfeasance or want of the care the law demands.[13] A data incident alone does not establish breach of duty. What matters is process: whether the board had a risk framework, asked the right questions and acted on the answers.

B. Risk oversight obligations of boards and committees

The Companies Act builds risk oversight into board structure. Schedule IV expects independent directors to satisfy themselves that systems of risk management are robust and defensible. For listed entities the SEBI LODR Regulations are more specific. Material events must be disclosed to the stock exchanges within prescribed timelines.[14] The Business Responsibility and Sustainability Report, required of the same top entities, calls for disclosure under the consumer-engagement principle of the number of data breaches, data-privacy complaints and the entity's cyber-security policy, drawing on the Ministry of Corporate Affairs' 2019 National Guidelines on Responsible Business Conduct.[15] These instruments turn data-protection performance into disclosed, auditable information. A leak preceded by silence in the board's minutes and in the BRSR invites both regulatory and shareholder scrutiny. SEBI's insider trading rules add another layer: information about a significant breach may be unpublished price sensitive information, so the board must manage trading windows and disclosures around an incident.[16]

C. A comparative standard of oversight

The most developed body of oversight doctrine comes from Delaware. In In re Caremark International Inc. Derivative Litigation the court recognised that directors may breach their duty by failing to make a good-faith attempt to put in place a reasonable information and reporting system, and in Marchand v. Barnhill the Delaware Supreme Court applied that duty

[13]Official Liquidator v P.A. Tendolkar, (1973) 1 SCC 602. The decision discusses circumstances in which directors may be held liable for misfeasance or neglect; it should not be read as imposing automatic liability for every corporate loss.

[14]Companies Act, 2013, sch IV, para II(4) (responsibilities of independent directors); Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, regs 17(9), 21 and 30, as applicable (risk-management and material-event disclosure requirements).

[15] (Listing Obligations and Disclosure Requirements) Regulations, 2015, reg 34(2)(f) and the prescribed Business Responsibility and Sustainability Report framework; Ministry of Corporate Affairs, National Guidelines on Responsible Business Conduct (2019). The precise disclosure requirements depend on the applicable reporting framework and category of listed entity.

[16]SEBI (Prohibition of Insider Trading) Regulations, 2015, reg 2(1)(n) (definition of unpublished price sensitive information) and reg 4 (prohibition on trading while in possession of such information), subject to the facts and applicable exceptions.

to a board with no committee or process for a central compliance risk.[17] Indian law has a statutory footing that is arguably stricter, because section 166(3) speaks of due and reasonable care and diligence and not merely good faith. No reported Indian decision known to the author applies it to a data-protection failure, which is a notable gap. Once DPDP penalties begin to be imposed, section 245 applications and derivative-style claims on the Caremark pattern appear likely.

CONCLUSION

Unauthorised sharing of customer data is no longer only an information-technology problem. It is a question of corporate governance, because it tests whether those who run a company have built systems that deserve the trust customers place in it. At the entity level, the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 make the company the single point of accountability as a Data Fiduciary.It must take reasonable security safeguards, and it must notify the Data Protection Board and affected customers of a breach. It remains answerable for its processors despite any contrary agreement. With penalties of up to ₹250 crore, the regime is serious enough to command board attention. The Significant Data Fiduciary provisions go further, requiring a Data Protection Officer who reports to the board. The Act is, however, incomplete as a system of accountability.

It also names no director or officer. Individual responsibility must therefore be traced through other laws: the Companies Act, 2013, under which directors owe duties of due care, skill and diligence under section 166 and the risk-oversight obligations of boards and audit committees apply; the SEBI listing regime, which requires risk management committees to address cyber security and demands disclosure of material events; and the criminal provisions of the IT Act, together with consumer protection law.

A prosecution or a shareholder claim must show what the individual knew, decided or neglected.

The practical lesson for boards is that the record of oversight matters as much as the technical controls. A board that can show a data-flow inventory, a committee with a clear mandate, regular reports from the Data Protection Officer, tested vendor contracts and a rehearsed incident-response plan is well placed to defend its decisions.

[17]In re Caremark International Inc Derivative Litigation, 698 A.2d 959 (Del Ch 1996); Marchand v Barnhill, 212 A.3d 805 (Del 2019). These Delaware decisions concern board oversight and compliance systems; their application in India would be comparative rather than binding.

For policymakers, the central challenge is alignment. Entity penalties, individual accountability and customer remedies currently sit in different statutes with different forums and standards. Clarifying the position of consumer commissions, considering a calibrated officer-liability provision, strengthening the independence of the Board and harmonising incident-reporting timelines would make the framework more coherent and more predictable.

The term “Data Fiduciary” implies a relationship of trust. For that trust to carry legal weight, India will need courts, regulators and boards that treat the protection of customer data as a duty owed to the customer and not merely a cost of doing business.