



“Who Owns the Corporate Data?”: Shareholder Rights Over High-Value Data Assets During Corporate Insolvency

*Aditya Mishra*¹, *Akshat Mishra*², *Md Saqib Ansari*³

¹ National Law Institute University, Bhopal

² National Law Institute University, Bhopal

³ National Law Institute University, Bhopal

ABSTRACT :

This paper examines shareholder rights over high-value corporate data assets during corporate insolvency in India. It investigates whether customer databases, proprietary datasets, behavioural information, algorithms, trained artificial-intelligence models, and related data infrastructure can be treated as corporate assets capable of transfer and monetisation during insolvency proceedings. The paper argues that corporate data cannot be reduced to a single category of property. Its legal and economic value depends upon ownership, control, contractual rights, confidentiality, processing authority, technological infrastructure, and the purposes for which personal data was collected. The analysis evaluates the relationship between the Companies Act, 2013, the Insolvency and Bankruptcy Code, 2016, and the Digital Personal Data Protection Act, 2023. It argues that shareholders do not possess a direct proprietary interest in corporate data merely because such data contributes to share value. However, they may possess important governance and remedial interests where directors seek to dispose of the company’s principal data undertaking, transfer data to related parties, or destroy enterprise value through an undervalued transaction. The paper further argues that a resolution applicant may acquire only the corporate debtor’s lawful and transferable interests in data. Insolvency approval cannot create unrestricted authority to process personal information. The paper concludes by proposing mandatory data-asset disclosure, privacy-sensitive valuation, shareholder safeguards, data-transfer schedules, and coordination among insolvency, company-law, data-protection, competition, and sectoral regulators.

Keywords: shareholder rights; corporate insolvency; data assets; Digital Personal Data Protection Act, 2023; Insolvency and Bankruptcy Code, 2016; Companies Act, 2013; data fiduciary; artificial intelligence; resolution applicant; privacy; data governance.

I. Introduction

Corporate wealth is increasingly generated by intangible resources rather than by land, machinery, or inventory. For many technology-driven companies, the principal sources of enterprise value are customer databases, proprietary datasets, behavioural profiles, algorithms, trained artificial-intelligence models, and the infrastructure through which these assets are collected and processed. These resources may determine a company’s market position, revenue-generation capacity, and attractiveness to investors. Yet, when such a company becomes insolvent, the legal character of its data-related assets remains uncertain. The central question is not merely whether data has monetary value, but who is entitled to control, transfer, and monetise that value.

The problem becomes particularly complex because “corporate data” is not a legally uniform category. A company may own a database structure or an algorithm, possess confidential business information, hold a contractual licence over a third-party dataset, or process personal data in its capacity as a data fiduciary. Under the Digital Personal Data Protection Act, 2023 (“DPDP Act”), a data fiduciary is the person who determines the purpose and means of processing personal data, while the data principal is the individual to whom that data relates.¹ Consequently, corporate control over information does not necessarily amount to unrestricted ownership of the personal data contained within a database.

This difficulty is intensified during insolvency. The Insolvency and Bankruptcy Code, 2016 (“IBC”) seeks the reorganisation and insolvency resolution of corporate persons in a time-bound manner, with the objective of maximising the value of assets and balancing the interests of stakeholders.² A resolution

¹ Digital Personal Data Protection Act, 2023, No. 22 of 2023, §§ 2(i), 2(j), India Code (2025), <https://www.indiacode.nic.in/bitstream/123456789/22037/2/a2023-22.pdf>.

² Insolvency and Bankruptcy Code, 2016, No. 31 of 2016, pmbli., India Code (2021), <https://www.indiacode.nic.in/bitstream/123456789/2154/5/A2016-31.pdf>.

professional or liquidator may therefore seek to preserve and transfer data-related assets as part of a going-concern sale, resolution plan, or liquidation process. However, the commercial value of such assets may depend on processing activities that remain subject to statutory, contractual, privacy, and cybersecurity obligations.

The Companies Act, 2013 provides a partial governance framework. Section 180(1)(a) requires shareholder approval for the sale, lease, or disposal of the whole or substantially the whole of an undertaking.³ Nevertheless, it is unclear whether this provision adequately addresses a company whose principal undertaking consists of data and data-derived technologies. Shareholders own shares rather than the company's underlying assets, but they may possess important governance and value-protection interests where directors seek to dispose of the company's core data infrastructure.

This paper argues that corporate data should be understood as a conditional corporate asset. Its economic value may belong to the company, but its collection, transfer, and subsequent use remain limited by shareholder-governance principles, insolvency law, privacy obligations, and the rights of data principals. The paper examines whether existing company-law concepts can effectively regulate this emerging asset class during corporate insolvency.

II. Conceptualising Corporate Data as an Asset Class

Corporate data should not be treated as a single, homogeneous form of property. In a data-intensive enterprise, value may be distributed across customer databases, transaction records, behavioural profiles, proprietary datasets, software code, algorithms, trained artificial-intelligence models, and the contractual relationships that permit access to or use of these resources. Each category may attract a different legal treatment. A database may contain personal data, while its structure may be protected through copyright, contract, confidentiality, or trade-secret principles. Similarly, an algorithm may be protected as software, confidential information, or an independently valuable business method. The legal analysis must therefore distinguish the information itself from the systems, rights, and relationships through which that information generates value.

The first distinction is between personal and non-personal data. Personal data concerns an identifiable individual, whereas non-personal data may consist of aggregated statistics, anonymised information, industrial information, or internally generated business intelligence. The Digital Personal Data Protection Act, 2023 ("DPDP Act") defines personal data by reference to an identifiable individual and treats collection, storage, use, sharing, disclosure, and erasure as forms of processing.⁴ Consequently, a company may exercise substantial commercial control over a customer database without possessing an unrestricted proprietary right over every item contained in it. Its legal position may instead resemble that of a data fiduciary, namely, an entity determining the purpose and means of processing personal data.⁵

The second distinction is between ownership, control, economic value, and lawful usability. Ownership concerns whether the company possesses a legally recognised proprietary or contractual interest. Control concerns the ability to access, modify, store, license, or transfer the asset. Economic value concerns the contribution of the asset to revenue, goodwill, market power, or enterprise valuation. Lawful usability concerns whether the asset can legally be used for a particular purpose. These concepts may diverge. For example, a company may control a customer database and derive significant revenue from it, but its ability to transfer the database to a purchaser may be restricted by privacy obligations, customer contracts, licensing conditions, or duties of confidentiality.

Corporate data is therefore better understood through a bundle-of-rights approach. The relevant rights may include access, possession, storage, analysis, licensing, commercial exploitation, retention, deletion, and transfer. A company may hold some of these rights without holding all of them. A licensed dataset, for example, may be commercially valuable but incapable of assignment without the licensor's consent. Likewise, an AI model may be transferable as software while the personal data used to train it remains subject to separate legal restrictions.

This approach also clarifies the relationship between data and conventional corporate assets. Data may function like intellectual property, inventory, goodwill, confidential information, or a contractual entitlement, depending on its source and use. Indian copyright law recognises copyright in eligible original works and permits assignment subject to statutory requirements, but copyright protection does not automatically confer ownership over facts or

³ Companies Act, 2013, No. 18 of 2013, § 180(1)(a), India Code (2026), <https://www.indiacode.nic.in/bitstream/123456789/2114/5/A2013-18.pdf?v=20260605114304>.

⁴ Digital Personal Data Protection Act, 2023, No. 22 of 2023, §§ 2(h), 2(t), 2(x), India Code (2025), <https://www.indiacode.nic.in/bitstream/123456789/22037/2/a2023-22.pdf>.

⁵ Id. § 2(i).

personal information contained in a compilation.⁶ The value of a dataset may instead arise from the effort of collection, organisation, verification, exclusivity, or the surrounding technological infrastructure.

Accordingly, “corporate data” should be treated as a conditional corporate asset class. Its value belongs to the enterprise only to the extent that the company possesses transferable rights in the relevant data or data-derived system. During insolvency, the asset must therefore be valued not merely by volume or commercial usefulness, but also by provenance, contractual assignability, privacy restrictions, security obligations, and the lawful purposes for which it may be processed.

III. Shareholder Rights Under Company Law

A. Transfer Separate Legal Personality

The starting point for analysing shareholder rights over corporate data is the doctrine of separate legal personality. Upon incorporation, a company becomes a body corporate capable of acquiring, holding, and disposing of property in its own name.⁷ The company is therefore legally distinct from its members, directors, and controlling shareholders. Its assets belong to the company as a separate juristic person, even where one shareholder owns the entire share capital.

This principle applies equally to data-related assets. A shareholder does not ordinarily own the company’s customer database, source code, proprietary datasets, goodwill, artificial-intelligence models, or the proceeds generated from their sale. The Supreme Court has repeatedly recognised that shareholders own shares in the company, not the property of the company itself.⁸ A shareholder may receive dividends or participate in residual assets after lawful satisfaction of corporate liabilities, but that interest does not amount to a present proprietary claim over any particular corporate asset.

The distinction is especially important in insolvency. The economic value of a company’s data may affect the value of its shares, but an indirect effect on share value does not give shareholders the right to prevent every transfer of that data. Any shareholder claim must therefore arise from corporate governance rights, fiduciary obligations, statutory remedies, or an unlawful diversion of corporate assets, rather than from direct ownership.

B. Directors’ Powers and Fiduciary Duties

The Companies Act, 2013 vests the board with authority to manage the company’s affairs and exercise its corporate powers, subject to the Act, the memorandum, the articles, and shareholder resolutions.⁹ Directors must exercise these powers in good faith for the benefit of the company, its members, employees, shareholders, and the community, while exercising due and reasonable care, skill, and diligence and avoiding situations involving direct or indirect conflicts of interest.¹⁰

These duties have particular significance where data constitutes the company’s principal source of value. A board may ordinarily decide to sell, licence, or commercialise data-related assets as part of the company’s business. That power is not unlimited. A transaction may be legally vulnerable where directors:

- Transfer a valuable database to a related party at an undervalue.
- Dispose of the company’s principal revenue-generating asset without a reliable valuation.
- Conceal material privacy, licensing, or contractual restrictions from the board or shareholders.
- Use impending insolvency to divert data or algorithms to a connected enterprise.
- Treat personal data as unrestricted corporate property.
- Approve a transaction in which the directors or their associates possess an undisclosed interest.

The relevant inquiry is not whether shareholders would have made a different commercial decision. It is whether the directors acted for a proper corporate purpose, on an informed basis, without conflict, and in a manner consistent with the company’s interests. A data transaction may therefore be

⁶ Copyright Act, 1957, No. 14 of 1957, §§ 13, 18, India Code, <https://www.indiacode.nic.in/indiacode/bitstream/123456789/1367/1/A195714.pdf>.

⁷ Companies Act, 2013, No. 18 of 2013, § 9, India Code (2026), <https://www.indiacode.nic.in/bitstream/123456789/2114/5/A2013-18.pdf?v=20260605114304>.

⁸ *Bacha F. Guzdar v. Comm’r of Income Tax*, 1955 S.C.R. 876, 884–85 (India); *Rustom Cavasjee Cooper v. Union of India*, (1970) 1 S.C.C. 248, 286–87 (India).

⁹ Companies Act § 179.

¹⁰ Id. § 166(2)–(4).

commercially unsuccessful without being legally improper. Conversely, a transaction that produces short-term liquidity may still breach directors' duties if it transfers the company's core data infrastructure to an associated entity for inadequate consideration.

C. Section 180 and Disposal of an Undertaking

Section 180(1)(a) of the Companies Act requires the board to obtain the company's consent through a special resolution before selling, leasing, or otherwise disposing of the whole or substantially the whole of an undertaking.¹¹ An "undertaking" includes one in which the company's investment exceeds twenty per cent of its net worth or one which generates twenty per cent of the company's total income. "Substantially the whole" refers to twenty per cent or more of the value of the undertaking, as reflected in the audited balance sheet of the preceding financial year.¹²

The provision can potentially apply where a company's data platform is its principal undertaking. If the database, analytical infrastructure, algorithms, and AI models collectively generate the company's central income or represent the principal investment of the enterprise, their disposal should ordinarily require shareholder approval. The board should not be able to avoid section 180 merely by describing the transaction as a licence, data partnership, technology transfer, outsourcing arrangement, or strategic collaboration. The substance and economic effect of the transaction should prevail over its contractual label.

This does not mean that every transfer of information requires a special resolution. The sale of a minor dataset in the ordinary course of business may fall outside section 180. The difficulty lies in applying a largely financial test to assets whose value may be strategic, future-oriented, or reflected in goodwill rather than current income. Data may also be deliberately undervalued on the balance sheet because accounting standards do not fully capture internally generated information and data-derived capabilities. Courts and regulators should therefore examine the asset's functional importance to the business, not merely its book value.

D. Shareholder Approval and Its Limits

Shareholder approval provides a governance safeguard, but it does not transform shareholders into owners of the underlying dataset. A special resolution authorises a corporate transaction; it does not transfer title in corporate property to the members. Nor does approval automatically validate a transaction that is fraudulent, based on material non-disclosure, or contrary to mandatory privacy and insolvency law.

The effectiveness of shareholder approval may also be limited by practical problems. Shareholders may receive incomplete information regarding data provenance, privacy restrictions, licensing conditions, or the consequences of transferring an AI model. The valuation of data may be uncertain, minority shareholders may be outvoted, and financial statements may not reveal the legal constraints attached to personal data. A transaction approved before insolvency may consequently remain open to challenge if it was undervalued, entered into with a related party, or designed to defeat creditors.

E. Oppression, Mismanagement, and Derivative Remedies

Sections 241 and 242 provide an additional protection where the company's affairs are conducted in a manner oppressive to members or prejudicial to the company, its members, or the public interest.¹³ Depending on the facts, the National Company Law Tribunal may regulate the company's future affairs, modify or terminate certain arrangements, or grant other appropriate relief. A shareholder may rely on these provisions where directors divert a core dataset to a connected entity, suppress material information, or conduct a conflicted sale that substantially diminishes corporate value.

Possible relief may include setting aside or restraining a conflicted transaction, requiring further disclosure, directing an independent valuation, regulating the company's affairs, or preventing the diversion of data to a related party. However, these remedies remain corporate and governance-based. They protect the company and its members against abuse of managerial power, but they do not confer ownership of personal data upon shareholders. The ultimate legal position is therefore one of differentiated interests: the company controls its lawful corporate assets, shareholders exercise governance and value-protection rights, directors owe fiduciary duties, and data principals retain independent statutory interests in the processing of their personal information.

¹¹ Id. § 180(1)(a).

¹² Id. § 180(1), Explanation (i)–(ii).

¹³ Id. §§ 241–242.

IV. Shareholders, Beneficial Interest, and Data-Generated Value

A. No Direct Proprietary Interest

Shareholders do not automatically own corporate data merely because that data increases the value of their shares. The separate legal personality of a company means that the company, and not its members, owns its assets and undertakes its liabilities. In *Bacha F. Guzdar v. Commissioner of Income Tax*, the Supreme Court held that a shareholder has no interest in the property of the company, although the shareholder may participate in profits when the company lawfully declares dividends.¹⁴ This principle applies equally to customer databases, proprietary datasets, algorithms, trained AI models, goodwill, and proceeds received from their sale.

The shareholder's legal interest is instead represented by a bundle of statutory and economic rights. These may include voting rights on company resolutions, the right to receive dividends when declared, the right to participate in residual assets after prior claims are satisfied, and the right to invoke statutory remedies in appropriate circumstances.¹⁵ None of these rights creates a proprietary claim over a particular corporate asset. The fact that a valuable dataset enhances share prices therefore gives shareholders an indirect economic interest, not legal ownership of the data.

This distinction is especially important during insolvency. Shareholders cannot ordinarily demand that a data asset be preserved for their personal benefit or veto its sale merely because its disposal may reduce the value of their shares. Their claim is against the company's management or the legality of the transaction, not against the data as their individual property.

B. Equitable and Governance-Based Interests

Although shareholders lack a proprietary interest, they may possess a significant governance-based interest in the preservation of enterprise value. Directors cannot use their statutory powers to destroy or transfer the company's core value for an improper purpose. A transaction involving a company's principal data platform may therefore be challenged where it is entered into at an undervalue, benefits a related party, or materially alters the company's business without adequate disclosure.

This interest is particularly relevant to minority shareholders. They may object to the extraction of data-generated value by controlling shareholders or directors through related-party arrangements. Where a company's business model has consistently depended on responsible management and commercial exploitation of a data platform, a sudden transfer of that platform to an associated entity may support an allegation of oppressive or prejudicial conduct under sections 241 and 242 of the Companies Act, 2013.¹⁶ In suitable cases, the company's data strategy may also form part of the factual background relevant to legitimate expectations, especially where management decisions substantially defeat the basis on which minority investors entered the company.

However, the equitable interest remains derivative and governance-based. It protects the company's value and the fairness of corporate decision-making. It does not convert shareholders into co-owners of personal data or confer upon them the right to determine how data principals' information should be processed.

C. Shareholder Value at Insolvency

The commencement of insolvency further limits shareholder influence. The IBC prioritises resolution, preservation of the corporate debtor as a going concern, and maximisation of value for stakeholders. Under the liquidation waterfall in section 53, equity shareholders rank after insolvency costs, secured and unsecured creditors, government dues, and other specified claims.¹⁷ Shareholders therefore generally receive value only after prior claims have been satisfied. They do not possess an ordinary veto over a resolution plan approved through the statutory process.

Shareholders nevertheless remain relevant to a data-intensive insolvency. Data may be the only asset capable of supporting a going-concern resolution. An undervalued sale of a database or AI platform may prejudice creditors as well as shareholders. The resolution process must also distinguish lawful value maximisation from unauthorised exploitation of personal data. Existing shareholders may possess important information regarding data provenance,

¹⁴ *Bacha F. Guzdar v. Comm'r of Income Tax*, 1955 S.C.R. 876, 884–85 (India), <https://indiankanoon.org/doc/1873699/>.

¹⁵ Companies Act, 2013, No. 18 of 2013, §§ 47, 52, 123, India Code (2026), <https://www.indiacode.nic.in/bitstream/123456789/2114/5/A2013-18.pdf?v=20260605114304>.

¹⁶ Companies Act §§ 241–242.

¹⁷ Insolvency and Bankruptcy Code, 2016, No. 31 of 2016, § 53, India Code (2021), <https://www.indiacode.nic.in/bitstream/123456789/2154/5/A2016-31.pdf>.

customer contracts, licensing restrictions, privacy representations, cybersecurity incidents, and the company's historical processing practices.

Their proper role is therefore not that of data owners. It is the role of stakeholders capable of identifying misconduct, preserving information, and questioning transactions that fail to reflect the company's lawful data-generated value.

V. Insolvency Law and Transfer of Data Assets

A. The IBC's Resolution Objective

The Insolvency and Bankruptcy Code, 2016 ("IBC") is structured around resolution rather than the immediate break-up of the corporate debtor. Its objectives include preserving the value of the corporate debtor, facilitating resolution as a going concern, and maximising the value of available assets for the benefit of stakeholders.¹⁸ These objectives are particularly significant where the company's principal value lies in intangible resources such as customer databases, proprietary datasets, algorithms, AI models, and data-processing infrastructure.

The IBC does not contain a comprehensive statutory regime specifically governing corporate data. Nevertheless, its reference to assets, records, information, intellectual property, contractual rights, and going-concern value is sufficiently broad to include many forms of data-related value. The principal difficulty is that the economic value of data may arise from a combination of ownership, possession, confidentiality, contractual access, processing rights, and business relationships. The resolution professional must therefore determine not simply whether information exists in the corporate debtor's systems, but whether the debtor possesses a transferable legal or commercial interest in it.

During the corporate insolvency resolution process, the interim resolution professional is required to take custody and control of the assets, records, documents, and other relevant information of the corporate debtor.¹⁹ The resolution professional must also collect information relating to the assets, liabilities, operations, financial position, and business affairs of the corporate debtor and prepare an information memorandum for prospective resolution applicants.²⁰ Section 29 further requires access to relevant information to be accompanied by undertakings concerning confidentiality, protection of intellectual property, and restrictions on disclosure to third parties.²¹ These safeguards are directly relevant to data-intensive insolvencies because the information memorandum may itself contain valuable personal data, trade secrets, source code, customer information, and commercially sensitive model architecture.

The Insolvency and Bankruptcy Board of India ("IBBI") regulations supplement this framework through provisions concerning information memoranda, confidentiality undertakings, valuation reports, and access to information. The regulations require the information memorandum to contain details of the corporate debtor's assets and liabilities that are necessary for assessing their value, while also requiring confidentiality protections for information shared with committee members and resolution applicants.²² Because the IBBI framework is periodically amended, the regulations applicable on the relevant insolvency commencement date must be identified rather than assumed.²³

B. Is Data an Asset of the Corporate Debtor?

Physical possession of data does not conclusively establish that the data forms part of the corporate debtor's transferable asset pool. A classification test should therefore be applied.

First, the resolution professional should ask whether the information was generated, acquired, or lawfully obtained by the company. Secondly, the company's contractual or statutory authority to collect and process the information must be identified. Thirdly, it must be determined whether the information is held for the company's own purposes or on behalf of a customer, licensor, service provider, or another organisation. Fourthly, the analysis should examine whether the information is subject to a trust, agency, bailment, confidentiality obligation, data-processing arrangement, or other limitation.

¹⁸ Insolvency and Bankruptcy Code, 2016, No. 31 of 2016, pmbi., India Code (2021), <https://www.indiacode.nic.in/bitstream/123456789/2154/5/A2016-31.pdf>.

¹⁹ Id. §§ 17–18.

²⁰ Id. § 25(1)–(2).

²¹ Id. § 29(2).

²² Insolvency and Bankruptcy Board of India (Insolvency Resolution Process for Corporate Persons) Regulations, 2016, reg. 36, [https://ibbi.gov.in/uploads/legalframework/IBBI_\(Insolvency_Resolution_Process_for_Corporate_Persons\)Regulations,_2016_updated_25.07.2019.pdf](https://ibbi.gov.in/uploads/legalframework/IBBI_(Insolvency_Resolution_Process_for_Corporate_Persons)Regulations,_2016_updated_25.07.2019.pdf).

²³ Insolvency and Bankruptcy Board of India, Legal Framework: Updated Regulations, <https://ibbi.gov.in/legal-framework/updated>.

The fifth question concerns assignability. A database may be commercially valuable but incapable of transfer without the consent of a licensor or contractual counterparty. The final question is whether the proposed transfer would alter the purpose for which personal data was collected. A purchaser cannot assume that acquiring a corporate database automatically permits every future use of the personal data contained in it.

This approach is consistent with the IBC's treatment of third-party assets. Section 36 excludes from the liquidation estate assets owned by third parties but held by the corporate debtor under trust, contractual arrangements, or bailment. It also excludes assets of an Indian or foreign subsidiary of the corporate debtor.²⁴ Therefore, information held by a company merely as a processor, custodian, agent, trustee, or service provider should not automatically be treated as an asset available for sale to satisfy corporate debts.

C. Resolution Plan Versus Asset Sale

The legal consequences of a data transaction depend partly on its structure. A sale of the entire business as a going concern is different from the sale of a standalone database. A going-concern resolution may transfer the data platform together with customer contracts, employees, compliance systems, security infrastructure, and the business purpose that originally justified processing the data. This structure is more likely to preserve continuity and reduce the risk of incompatible use.

By contrast, a standalone database sale may separate personal information from the customer relationship, privacy notices, internal controls, and processing purpose that supported its original collection. The following transactions should therefore be distinguished:

- A going-concern transfer of the entire business.
- Transfer of a data platform together with assignable contracts.
- Sale of an isolated customer or behavioural database.
- Licensing of an AI model or algorithm.
- Sale of servers, storage systems, or database infrastructure.
- Transfer of shares in a subsidiary that holds or manages the data.

Each transaction may involve a different combination of ownership, control, processing authority, and contractual assignability. A resolution plan should describe these components separately rather than referring generally to the "sale of data assets."

D. Can a Resolution Applicant Acquire Data?

A resolution applicant may acquire the corporate debtor's lawful rights in data-related assets, but it does not acquire an unrestricted licence to process every item of information contained in those assets. The purchaser may acquire database architecture, anonymised or aggregated datasets, software, algorithms, trade secrets, confidential information, model weights, and assignable customer contracts. It may also assume the company's operational role as a data fiduciary, but that role remains subject to continuing obligations under applicable data-protection law.

The purchaser may not automatically acquire personal data for an incompatible purpose, information held on behalf of another organisation, data subject to deletion or withdrawal obligations, third-party licensed datasets whose contracts prohibit assignment, or information collected unlawfully or without legally adequate notice. Approval of a resolution plan should therefore be understood as authorising the transfer of the debtor's legally transferable interests, not as curing defects in the original collection or creating new permission for unlawful processing.

E. Due Diligence and Valuation

Every data-intensive insolvency should include a detailed data asset schedule. It should identify the categories of data, source and provenance, legal basis for collection and processing, consent or notice architecture, retention periods, outstanding data-principal requests, cross-border storage or transfers, security incidents, contractual assignment restrictions, and the status of the information as personal, anonymised, pseudonymised, or non-personal data. The schedule should also identify dependencies between datasets, algorithms, model weights, software, and customer contracts.

Valuation should incorporate a compliance discount. A dataset with high commercial usefulness but significant privacy, licensing, cybersecurity, or contractual restrictions should not be valued as if it were freely transferable property. The proper value of a data asset is therefore its expected economic benefit minus the cost and legal risk associated with lawful use. This approach aligns insolvency valuation with the central proposition of this paper: data may be a corporate asset, but its value is conditional upon the company's ability to use and transfer it lawfully.

²⁴ Insolvency and Bankruptcy Code § 36(4)(a).

VI. DPDP Act and Limits on Transfer

A. Corporate Control Is Not Data-Subject Ownership

The Digital Personal Data Protection Act, 2023 (“DPDP Act”) creates a distinction between control over data processing and rights in the personal data of individuals. A company may act as the “Data Fiduciary” because it determines the purpose and means of processing, while the individual to whom the data relates remains the “Data Principal.”²⁵ The company may therefore control collection, storage, analysis, disclosure, and deletion, but this control does not convert personal data into unrestricted corporate property.

This produces a divided legal structure. The company exercises enterprise-level control over data systems and processing decisions. The data principal retains statutory rights concerning access, correction, updating, erasure, consent withdrawal, and grievance redressal.²⁶ An insolvency purchaser may become the new data fiduciary or assume the relevant processing function, but the transfer does not extinguish the data principal’s rights or retrospectively validate unlawful collection.

The DPDP Act also places responsibility on the data fiduciary for processing undertaken by a data processor. A contractual arrangement with a resolution professional, purchaser, cloud provider, or technology vendor cannot by itself transfer away the underlying statutory responsibility.²⁷ Accordingly, an insolvency sale may transfer databases, software, and business operations, but it must also identify the entity responsible for continuing compliance.

B. Purpose Limitation and Lawful Processing

The purchaser’s proposed use must be examined against the purpose for which the data was originally collected. Under section 4, personal data may be processed only for a lawful purpose based on consent or a recognised legitimate use.²⁸ The consent requirement is linked to a specified purpose and must be free, specific, informed, unconditional, and unambiguous.²⁹ The accompanying notice must identify the personal data and the purpose for which it is proposed to be processed.³⁰

This creates a significant distinction between continuity and repurposing. A purchaser acquiring a customer database to continue providing the same services may be able to justify continued processing, subject to the applicable statutory requirements. The position is more difficult where the purchaser acquires the same database to sell unrelated behavioural profiles, conduct targeted advertising, or train a new commercial AI model. The fact that both activities generate revenue does not make them legally equivalent.

The resolution professional and resolution applicant should therefore assess:

- The original purpose of collection.
- The contents of the notice given to data principals.
- Whether consent was obtained and can be demonstrated.
- Whether processing falls within a statutory legitimate use.
- Whether the proposed use is materially different from the original use.
- The sensitivity and potential impact of the processing.
- The reasonable expectations of affected data principals.
- Any contractual or sectoral restrictions governing the information.

The transfer of a corporate database should not be treated as an automatic assignment of every possible purpose of processing.

C. Retention, Erasure, and Accuracy

The DPDP Act imposes continuing obligations concerning data accuracy, security, breach notification, retention, and erasure. Where personal data is likely to be used to make a decision affecting the data principal or disclosed to another data fiduciary, the processing entity must ensure its completeness,

²⁵ Digital Personal Data Protection Act, 2023, No. 22 of 2023, §§ 2(i), 2(j), India Code (2025), <https://www.indiacode.nic.in/bitstream/123456789/22037/2/a2023-22.pdf>.

²⁶ Id. §§ 6(4), 11–13.

²⁷ Id. § 8(1)–(2).

²⁸ Id. § 4.

²⁹ Id. § 6(1).

³⁰ Id. § 5(1).

accuracy, and consistency.³¹ It must also adopt reasonable security safeguards and notify the Data Protection Board and affected data principals in the event of a personal-data breach.³²

Section 8(7) requires erasure when the data principal withdraws consent or when it is reasonable to assume that the specified purpose is no longer being served, unless retention is necessary under another law.³³ Section 12 separately recognises rights to correction, completion, updating, and erasure, subject to retention necessary for the specified purpose or legal compliance.³⁴ These duties create a direct tension with insolvency valuation. The resolution professional may seek to preserve every item of information in order to maximise the sale price, while the data-protection framework may require deletion, restriction, or correction.

“Preserving value” cannot therefore mean preserving unlawfully retained personal data. A dataset containing stale, unlawfully obtained, or deletion-sensitive information may have a lower lawful value than its raw volume suggests. Its valuation must reflect the cost of compliance and the data that must be removed before transfer.

D. Transfer to the Resolution Applicant

A legally sound resolution plan should adopt a three-stage model.

First, a pre-transfer assessment should identify which data can lawfully be disclosed to bidders, transferred to the successful applicant, or retained by the corporate debtor. Sensitive personal data should be segregated from anonymised, aggregated, non-personal, and proprietary business information.

Secondly, the transaction should involve a conditional transfer. The resolution applicant should receive only the data and rights necessary for the approved business purpose. The resolution plan should specify the purpose, categories of information, permitted users, retention period, security arrangements, and restrictions on onward disclosure.

Thirdly, the purchaser should be subject to post-transfer supervision. It should provide appropriate notices where required, honour consent withdrawals and erasure requests, maintain processing records, preserve security safeguards, and establish an effective grievance mechanism.

The resolution plan should expressly allocate responsibility for:

- Data-principal access, correction, and erasure requests.
- Historical and post-transfer data breaches.
- Regulatory notices and investigations.
- Deletion and retention obligations.
- Data-processing agreements.
- Cybersecurity and audit expenses.
- Costs arising from unlawful historical collection.
- Responsibility for data held by processors or third-party vendors.

Section 17(1)(e) provides a relevant statutory context by excluding certain DPDP Act provisions where processing is necessary for an approved scheme of compromise, arrangement, merger, reconstruction, or transfer of undertaking. However, this provision should not be read as a general exemption for every IBC transaction. Its language is directed to specified corporate restructuring transactions approved by a competent authority, and the continuing obligations under section 8(1) and section 8(5) remain important.³⁵ In any event, an exemption concerning processing during an approved transaction should not be treated as unrestricted permission for all subsequent commercial uses.

E. Personal Data, Anonymisation, and AI Models

Trained AI models create a further conceptual difficulty. The model weights may be stored separately from the training database and may not display

³¹ Id. § 8(3).

³² Id. § 8(4)–(6).

³³ Id. § 8(7).

³⁴ Id. § 12.

³⁵ Id. § 17(1)(e).

personal information in an immediately readable form. Nevertheless, a model may encode patterns derived from personal data, reproduce memorised information, enable re-identification, or produce outputs that affect identifiable individuals.

Before transferring model weights, the resolution process should ask:

- Was the training data lawfully collected and processed?
- Was model training within the specified purpose communicated to data principals?
- Does the model permit extraction or memorisation of personal information?
- Can the model be transferred without transferring the underlying dataset?
- Does the purchaser's new purpose constitute materially different processing?
- Are the model weights subject to software licences, confidentiality duties, or third-party restrictions?
- Should a separate audit assess provenance, re-identification, and security risks?

Anonymisation should not be treated as an automatic solution. The relevant question is whether the information can reasonably be linked to identifiable individuals, directly or through technical means. The correct legal approach is therefore to subject model weights, training datasets, and derived outputs to separate technical and legal assessments.

The DPDP Act does not make insolvency impossible. It requires insolvency actors to recognise that data value is conditional. A resolution applicant may acquire a lawful data-enabled business, but it cannot acquire an unrestricted licence to exploit personal information beyond the legal purposes, rights, and safeguards that accompany the transfer.

VII. The Boundary Between Companies Act, IBC, and DPDP Law

The regulation of corporate data during insolvency cannot be assigned to a single statute. The Companies Act, 2013, the Insolvency and Bankruptcy Code, 2016 ("IBC"), and the Digital Personal Data Protection Act, 2023 ("DPDP Act") address different legal dimensions of the same transaction. The Companies Act is principally concerned with corporate authority and managerial accountability. The IBC governs the preservation, valuation, and resolution of the corporate debtor's assets. The DPDP Act regulates the lawful processing of digital personal data and protects the interests of data principals.³⁶

The Companies Act operates primarily before and alongside insolvency. It determines whether directors possessed authority to dispose of a data platform, whether shareholder approval was required under section 180, and whether the transaction involved oppression, mismanagement, conflict of interest, or diversion of corporate value under sections 241 and 242.³⁷ Its central question is whether the company's internal decision-making was properly authorised and fairly conducted.

The IBC addresses a different question: how should the corporate debtor's lawful interests be preserved and transferred for the purpose of resolution? The resolution professional takes control of the corporate debtor's assets, records, and business information, prepares the information memorandum, and facilitates the submission and evaluation of resolution plans.³⁸ The committee of creditors and the adjudicating authority then assess whether the proposed plan satisfies the statutory requirements and maximises value. Shareholder approval cannot ordinarily operate as a separate veto once the transaction is governed by the insolvency process.

The DPDP Act imposes an independent limitation. It determines whether personal data may be collected, retained, disclosed, transferred, or used for the purchaser's proposed purpose. Approval under the IBC does not automatically authorise processing that would otherwise violate the DPDP Act. Similarly, compliance with the DPDP Act does not by itself establish that directors complied with their Companies Act duties or that the transaction provides adequate value to creditors.

³⁶ Companies Act, 2013, No. 18 of 2013, §§ 166, 180, 241–242, India Code (2026), <https://www.indiacode.nic.in/bitstream/123456789/2114/5/A2013-18.pdf?v=20260605114304>; Insolvency and Bankruptcy Code, 2016, No. 31 of 2016, §§ 18, 25, 29–31, India Code (2021), <https://www.indiacode.nic.in/bitstream/123456789/2154/5/A2016-31.pdf>; Digital Personal Data Protection Act, 2023, No. 22 of 2023, §§ 4–8, India Code (2025), <https://www.indiacode.nic.in/bitstream/123456789/22037/2/a2023-22.pdf>.

³⁷ Companies Act §§ 166, 180, 241–242.

³⁸ Insolvency and Bankruptcy Code §§ 18, 25, 29–31.

These statutes should therefore be read functionally rather than hierarchically. The Companies Act governs corporate authority, fiduciary conduct, and shareholder protection. The IBC governs insolvency administration, asset valuation, resolution, and distribution. The DPDP Act governs the lawful processing of personal data before, during, and after the transaction. Contract, intellectual-property, competition, and sector-specific laws may add further restrictions.

The most coherent approach is to treat insolvency approval as authorising only the transfer of legally transferable corporate interests. A resolution plan should identify the data being transferred, the purpose of post-transfer processing, the purchaser's compliance obligations, and responsibility for historical breaches and data-principal requests. Courts should maximise lawful value, not merely the nominal sale price of information. In this framework, the IBC cannot be used to erase privacy rights, the DPDP Act cannot be used to disregard legitimate insolvency value, and the Companies Act cannot be treated as conferring direct ownership of corporate data upon shareholders.

VIII. Proposed Reform Framework

A. Statutory Recognition of Data Assets

Indian company and insolvency law should expressly recognise data-related assets while avoiding the assumption that all data is owned by the corporate debtor. The legislation or IBBI regulations should distinguish between corporate-owned or licensed data, personal data held under fiduciary control, third-party data held under trust or contract, anonymised and aggregated datasets, and AI models or derived datasets.

This classification would clarify what can be transferred, what requires consent or contractual approval, and what must remain outside the insolvency estate. It would also distinguish ownership of a database structure or model from the limited authority to process the information contained within it.

B. Mandatory Data Asset Disclosure

Data-intensive companies should be required to maintain a data asset register and disclose material information in annual reports. During insolvency, the same information should form part of the information memorandum prepared under section 29 of the Insolvency and Bankruptcy Code, 2016 ("IBC"). Existing insolvency regulations already require disclosure of assets, liabilities, litigation, investigations, and other information relevant to valuation. The framework should expressly extend this disclosure to material data assets and associated legal restrictions.³⁹

The disclosure should identify:

- Principal data categories and their commercial significance.
- Material licences and assignment restrictions.
- Processing purposes and legal bases.
- Privacy, confidentiality, and sectoral restrictions.
- Data-related liabilities and pending data-principal requests.
- AI-model training provenance.
- Cybersecurity incidents and regulatory investigations.
- Estimated costs of retention, remediation, deletion, and compliance.

C. Shareholder Safeguards

Where data constitutes the company's core undertaking, disposal outside the ordinary course of business should require enhanced governance. Section 180 of the Companies Act, 2013 already requires a special resolution for the disposal of the whole or substantially the whole of an undertaking.⁴⁰ The law should clarify that the provision applies where a data platform, database, AI model, or related infrastructure represents the company's principal undertaking, even if its book value understates its strategic importance.

Additional safeguards should include independent valuation, audit-committee review, related-party scrutiny under section 188, disclosure of data-

³⁹ Insolvency and Bankruptcy Code, 2016, No. 31 of 2016, § 29, India Code (2021), <https://www.indiacode.nic.in/bitstream/123456789/2154/5/A2016-31.pdf>; Insolvency and Bankruptcy Board of India (Insolvency Resolution Process for Corporate Persons) Regulations, 2016, reg. 36,

[https://ibbi.gov.in/uploads/legalframework/IBBI_\(Insolvency_Resolution_Process_for_Corporate_Persons\)Regulations,_2016_updated_25.07.2019.pdf](https://ibbi.gov.in/uploads/legalframework/IBBI_(Insolvency_Resolution_Process_for_Corporate_Persons)Regulations,_2016_updated_25.07.2019.pdf).

⁴⁰ Companies Act, 2013, No. 18 of 2013, § 180(1)(a), India Code (2026), <https://www.indiacode.nic.in/bitstream/123456789/2114/5/A2013-18.pdf?v=20260605114304>.

protection consequences, and a fairness opinion where the transaction materially changes the company's business.⁴¹ These safeguards would protect shareholders against undervalued transfers without granting them direct ownership of the data.

D. Insolvency Safeguards

- Every resolution plan involving significant data assets should contain:
- A detailed data-transfer schedule.
- A privacy-impact and legality assessment.
- A compliance warranty from the resolution applicant.
- A protocol for data-principal rights.
- A retention, deletion, and correction plan.
- Allocation of liability for historical violations.
- Technical safeguards against unauthorised copying.
- Confidentiality obligations and access controls.

The plan should identify which data is transferred, for what purpose, under whose control, and subject to which restrictions. The purchaser should not receive a broader right of processing merely because the resolution plan has been approved.

E. Supervisory Coordination

Data-intensive insolvencies require institutional coordination among the National Company Law Tribunal, IBBI, the Data Protection Board, sectoral regulators, and the Competition Commission of India. NCLT should assess corporate and insolvency legality, IBBI should prescribe disclosure and valuation standards, and the Data Protection Board should address unlawful processing and data-principal rights. Competition authorities should examine transactions that create excessive concentration of datasets or data-driven market power.

The reform objective should be coordinated supervision, not overlapping control. The central principle should be that insolvency law may facilitate the transfer of lawful data-generated value, but it cannot convert restricted personal information into unrestricted property.

IX. Conclusion

Corporate data cannot be understood through a simple ownership model. A company may control databases, algorithms, AI models, trade secrets, and data-processing infrastructure, but that control does not mean that shareholders own the underlying information or that the company possesses an unrestricted right to exploit it. Corporate data is better understood as a composite and conditional asset. Its value depends upon the company's legal title, contractual rights, processing authority, confidentiality interests, technological infrastructure, and ability to use the data for a lawful purpose.

The separate legal personality principle prevents shareholders from claiming direct ownership over customer databases, proprietary datasets, goodwill, or AI models. Shareholders own shares and possess governance, voting, dividend, and statutory remedial rights. Where data constitutes the company's principal undertaking, however, those governance rights become significant. Section 180 of the Companies Act, 2013 may require shareholder approval for the disposal of the whole or substantially the whole of a data-intensive undertaking. Sections 241 and 242 may also provide remedies where directors transfer core data value to related parties, act for improper purposes, or conduct corporate affairs in a manner oppressive or prejudicial to members.⁴² These provisions protect corporate value and the integrity of decision-making, but they do not convert shareholders into owners of personal data.

The IBC introduces a further shift in priorities. During insolvency, the objective is to preserve the corporate debtor as a going concern and maximise lawful value for stakeholders. A resolution applicant may therefore acquire the corporate debtor's transferable rights in databases, software, algorithms, model weights, trade secrets, and related contracts. Yet, approval of a resolution plan cannot create rights that the corporate debtor never possessed. Third-party data held under trust, contract, agency, or processing arrangements cannot automatically be sold merely because it is physically stored in the debtor's systems.

⁴¹ Id. § 188.

⁴² Companies Act, 2013, No. 18 of 2013, §§ 180, 241–242, India Code (2026), <https://www.indiacode.nic.in/bitstream/123456789/2114/5/A2013-18.pdf?v=20260605114304>.

The DPDP Act establishes the most important limit on data monetisation. A purchaser may acquire a data-enabled business, but it does not receive an unrestricted licence to process personal data for every commercially attractive purpose. The purchaser must respect the original purpose of collection, applicable processing grounds, security obligations, retention duties, correction and erasure rights, and the continuing interests of data principals.⁴³ A resolution plan should therefore contain a data-transfer schedule, privacy assessment, compliance warranty, data-subject rights protocol, and clear allocation of liability for historical and future breaches.

The principal conclusion is that insolvency law should maximise lawful data-generated value, not merely the sale price of information. Data should be valued after accounting for privacy restrictions, contractual limits, provenance defects, cybersecurity risks, deletion obligations, and the cost of future compliance. The Companies Act, IBC, and DPDP Act should operate as complementary regimes: the Companies Act governs corporate authority and accountability, the IBC governs resolution and value distribution, and the DPDP Act governs the lawful processing of personal data.

The answer to the question “Who owns the corporate data?” is therefore necessarily plural. The company may hold enterprise-level control, shareholders hold governance interests, creditors hold insolvency claims, resolution applicants acquire only transferable rights, and data principals retain legally protected interests in the use of their personal information. Recognising these differentiated interests is essential if data is to become a legitimate corporate asset class without being reduced to unrestricted property available for sale to the highest bidder.

⁴³ Digital Personal Data Protection Act, 2023, No. 22 of 2023, §§ 4, 8, 12, India Code (2025), <https://www.indiacode.nic.in/bitstream/123456789/22037/2/a2023-22.pdf>.