CHANGE OF CONTROL UNDER CIRP: CHANGE OF CONTROL, CONTINUITY OF PROCESSING, AND PERSONAL DATA RIGHTS UNDER INDIAN INSOLVENCY LAW

Lakshay Arora & Khushi Sharma, Christ (Deemed to be University) Delhi NCR

ABSTRACT

This paper examines whether a successful Corporate Insolvency Resolution Process (CIRP) resulting in a change of control creates a fresh consent or renewed notice obligation under India's Digital Personal Data Protection Act, 2023 (DPDP Act). Existing commentary has addressed the monetisation of data assets in insolvency, but has not adequately confronted the prior and conceptually distinct question that does a material change in the identity of those who govern, direct and exploit personal data alter the legitimacy of continued processing. The paper argues for a hybrid position. Prior consent should not automatically lapse upon resolution, as a blanket reset would undermine going-concern value and impede legitimate rescue. However, where a resolution results in a material change of control, processing purpose, or data recipient, the incoming resolution applicant incurs renewed notice obligations and, in cases of genuinely new or incompatible use, a requirement to obtain fresh consent.

The paper through doctrinal analysis supported by comparative examples, and normative proposal, analyses the relevant provisions of the IBC and the DPDP Act, examines the Toysmart and RadioShack controversies in the United States and the GDPR framework in Europe as persuasive guides, and proposes a calibrated Indian framework built around a mandatory post-resolution notice obligation, a continuity safe harbour for operationally necessary processing, a material-change trigger for renewed consent, and better coordination between insolvency and data protection regulators.

Keywords: Corporate Insolvency Resolution Process, Consent, Data Fiduciary, Data Principal, Purpose Limitation, Personal Data Governance.

I. INTRODUCTION

Contemporary enterprises in lending, payments, e-commerce, and healthcare technology accumulate personal data at scale. That data i.e. structured records of identity, financial behaviour, and communication may underlyingly represent a significant component of enterprise value, sometimes dwarfing tangible assets on the balance sheet. When such an enterprise becomes insolvent, the question of what happens to personal data, and to the rights of the individuals behind it, is no longer peripheral.

Even where a business has exhausted its capital, lost operational assets, or ceased viable operations, one resource often remains as a commercially significant residue: customer data, increasingly capable of functioning as the new oil of the digital economy in the digital era. Yet, like oil, it cannot be allowed to flow unchecked, its misuse impose serious legal and social costs.

India's Corporate Insolvency Resolution Process, established under the Insolvency and Bankruptcy Code, 2016[1] (IBC), is designed to facilitate time-bound commercial rescue of the sinking businesses. A resolution plan, once approved by the National Company Law Tribunal (NCLT) under Section 31[2] of the IBC, binds all stakeholders and vests a reconstituted enterprise in the resolution applicant. The corporate debtor survives as a legal entity. Its databases survive with it. The question this article addresses is whether the personal data those databases contain survives on the same legal terms.

The Digital Personal Data Protection Act, 2023[3] (DPDP Act) being the India's first comprehensive personal data protection legislation which is built around consent, notice and fiduciary accountability. It requires that personal data be processed only on the basis of free, specific, informed, and unambiguous consent, or pursuant to an enumerated legitimate use. It confers rights on Data Principal: the person whose data is processed, including rights to information, correction, erasure, and withdrawal of the consent.

The collision between these two regimes generates a concrete regulatory problem. The Supreme Court of India has recognised privacy as a fundamental right.[4] The DPDP Act

[1] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016 (India) [hereinafter IBC].
[2] IBC § 31
[3] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [hereinafter DPDP Act].
[4] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India)

operationalises that right in the commercial context. Yet neither statute squarely addresses what occurs when a CIRP resolution transfers effective governance of a data-intensive enterprise to an entirely new set of principals. Existing Indian commentary has examined the monetisation of data assets in insolvency proceedings, but has insufficiently addressed whether a successful CIRP resolution resulting in a change of control creates a fresh consent or renewed notice obligation under the DPDP Act framework. This is the research gap the paper addresses.

Three questions guide the analysis.

First, does change of control under a resolution plan change the legitimacy of continued data processing, independently of whether the corporate entity formally persists?

Second, does Section 31's binding effect on insolvency stakeholders displace independent obligations arising under another statute?

Third, how should Indian law calibrate the tension and intersection between insolvency rescue objectives and ongoing privacy compliance?

The methodology is doctrinal, comparative, and normative. The article maps the relevant statutory provisions, draws on persuasive comparative experience, and proposes a workable Indian framework. The remainder proceeds as follows. Section II analyses the CIRP structure and the significance of change of control. Section III examines the DPDP Act's consent and notice architecture. Section IV evaluates three competing models for whether CIRP creates a fresh consent event. Section V analyses the scope and limits of Section 31. Section VI surveys comparative guidance. Section VII offers a fintech illustration. Section VIII sets out the proposed framework, including a decision matrix. Section IX concludes.

II. CIRP, CONTROL CHANGE AND THE ASSET LOGIC OF PERSONAL DATA

A. CIRP Mechanics and Change of Control

Upon the admission of an insolvency application, an interim resolution professional (IRP) is appointed and assumes control of the corporate debtor's management.[5] The IRP takes custody of all assets, properties, and business records under Section 18[6] of the IBC. The corporate

[5] IBC §§ 16–17
[6] IBC § 18

debtor's operations are maintained as a going concern under Section 20[7], and the resolution professional (RP) who succeeds the IRP is obliged under Section 25[8] to preserve and protect those assets pending resolution.

A resolution plan submitted by an applicant must satisfy the minimum requirements of Section 30(2)[9] and, upon approval by the NCLT, becomes binding on all stakeholders under Section 31[10]. In a data-intensive enterprise, the approved plan typically transfers effective governance including board control, management rights, operational authority to the resolution applicant. The legal entity survives. Its company registration, contracts, and databases carry over. But the persons who determine what that entity does with personal data, its purpose, its means, its commercial strategy may be wholly different from those who held that position when individuals first provided their data.

The distinction between formal corporate continuity and substantive change of control is not a technical nicety. It goes to the heart of whether prior consent, given to a specific governing entity for specific purposes, can be said to authorise processing by a materially different set of decision-makers pursuing potentially different objectives.

B. Personal Data as: Enterprise Value versus Legal Relationship

A resolution applicant acquiring a data-intensive enterprise will often value the enterprise substantially by reference to its user base and data repositories. This is commercially unremarkable. But the commercial value of a database and the legal authority to exploit it are distinct things.

A database is a technical and commercial asset. The personal data within it is simultaneously the subject of legal rights held by each individual whose data appears there. Those rights to information, consent, correction, withdrawal, and erasure are not transferred when the enterprise is acquired, because they are held by the Data Principal, not by the corporate debtor. An incoming resolution applicant acquires the infrastructure of a data relationship; it does not, by that acquisition alone, inherit unrestricted authority over the personal data the infrastructure

[7] IBC § 20
[8] IBC § 25
[9] IBC § 30(2)
[10] IBC § 31(1)

contains.

This distinction is important precisely because it is easy to obscure. Insolvency proceedings treat data infrastructure as an asset to be preserved and maximised. Data protection law treats personal data as a matter of ongoing relationship, subject to continuing obligations. The two framings are not irreconcilable, but they must each be given effect.

III. THE DPDP ACT: CONSENT, NOTICE AND CONTINUING OBLIGATIONS

A. The Consent Architecture

Section 4[11] of the DPDP Act permits personal data to be processed only for a lawful purpose. Section 6[12] requires consent to be free, specific, informed, and unambiguous and must be given for a specified purpose. Section 7[13] enumerates legitimate uses for which separate consent is not required, including processing necessary for the performance of a contract to which the Data Principal is a party and processing required by law or court order.

Section 8[14] imposes continuing duties on the Data Fiduciary: to maintain accuracy, to implement security safeguards, to process data only for the stated purpose, and to respond to Data Principal requests. Section 11[15] confers on the Data Principal the right to withdraw consent at any time, though withdrawal does not affect the lawfulness of prior processing.

These provisions reflect a relational, purposive model of consent. A Data Principal's consent is given to an identified entity for an identified purpose in a particular context. This is consistent with the influential theory of contextual integrity, the idea that information flows are appropriate when they match the norms of the social setting in which the information was originally shared.[16]

B. Why Controller Identity Matters

The DPDP Act defines the Data Fiduciary as any person who determines the purpose and

[11] DPDP Act § 4
[12] DPDP Act § 6
[13] DPDP Act § 7
[14] DPDP Act § 8(1)–(7)
[15] DPDP Act § 11
[16] Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life 140–47 (Stanford Univ. Press 2010)

means of processing personal data. This definition tracks function rather than corporate form. When the resolution applicant acquires effective governance of the corporate debtor, it assumes the function of determining purpose and means. It thereby steps into the role of Data Fiduciary regardless of whether the registered company number has changed.

When the entity performing that function changes materially, through a change in controlling shareholder, governing board, strategic direction, or restructuring of the business itself, the individuals who provided data to the original entity may reasonably hold different expectations about how their data will be used. They may have trusted the original entity's brand, compliance record, or sector expertise. A post-resolution restructuring may also result in personal data being processed in ways materially different from those for which the user originally consented under the previous fiduciary or corporate framework. Consent, therefore, cannot be assumed to extend automatically to any entity that subsequently acquires corporate control.

The DPDP Act does not expressly address post-CIRP data processing. Nor does it contain a provision specifically governing changes of controller in business transfers. This silence, however, is not a licence. The Act's purposive consent architecture requires that processing remain consistent with the purpose for which consent was given, and that the Data Principal be kept informed of material developments. A change of effective control is precisely the kind of development that may require both.

IV. DOES SUCCESSFUL CIRP CREATE A FRESH CONSENT EVENT?

The present statutory framework does not provide us with an answer to this question. This leaves us with three possible approaches.

A. Model 1 – Continuity

The simplest position is that a successful CIRP creates no consent event of any kind. Since the corporate debtor survives as a legal entity, all pre-existing legal relationships including data processing authorisations carry over subject to the new control. The approved resolution plan is binding under Section 31 and has been held to preclude residual claims not addressed therein. On this view, requiring fresh consent would impose transaction costs that delay rescue, reduce bidder interest, and harm going-concern outcomes. These are not trivial concerns. In a competitive resolution market, even modest compliance obligations can discourage otherwise

viable bidders or reduce plan valuations.

However, the continuity model conflates legal entity survival with continuity of the consent relationship. Consent was given to a specific institutional identity for a specific purpose; the mere persistence of a company number does not preserve that alignment when governance, purpose, or recipient identity change substantially. Moreover, treating Section 31's binding effect as displacing independent obligations arising under separate legislation requires a textual basis that the IBC does not provide. Section 31 is directed at creditors, guarantors, and insolvency stakeholders but not at statutory rights held by individuals under a different enactment.

B. Model 2 – Successor Controller

At the other extreme, the successor-controller model holds that any change of control requires fresh consent from every Data Principal before any processing resumes. The logic is that the incoming resolution applicant is, for practical purposes, a new Data Fiduciary, and must independently establish a lawful basis for each processing activity.

This model is conceptually coherent and offers strong protection for Data Principals. However, it is operationally unworkable in the insolvency context. An enterprise may hold data belonging to hundreds of thousands of individuals. Universal fresh consent before any processing resumes would paralyse operations, prevent servicing of existing contractual obligations like loan repayments, insurance renewals, service subscriptions and destroy the going-concern value that CIRP is designed to preserve. The successor-controller model, applied universally, would effectively render data-intensive enterprises unresolvable, since no credible resolution applicant would accept a plan premised on a universal consent campaign of uncertain outcome.

C. Model 3 – Hybrid

The more defensible position distinguishes between processing that is necessary for genuine operational continuity and processing that constitutes a materially new or incompatible use of personal data.

First, processing that remains strictly necessary for the performance of existing contracts, the fulfilment of regulatory obligations, or the continuation of services actively in use by Data Principals falls within a continuity safe harbour. Prior consent survives for such processing,

because the Data Principal's reasonable expectation that his data be used for the purpose he originally agreed to is not disturbed by the change of control per se. What he is owed is timely notice that a new entity now governs the enterprise.

Second, where the resolution applicant intends to process personal data for purposes that are materially different from, or incompatible with, the original stated purpose such as cross-selling unrelated products, transferring data to affiliated analytics entities, or building new behavioural profiles the consent basis is not carried forward. Such processing requires either fresh consent or a legitimate use falling squarely within Section 7 of the DPDP Act.

Third, the notice obligation is universal. Regardless of whether the processing falls within the safe harbour, Data Principals should be informed, within a reasonable period after plan approval, that a new entity has assumed effective governance and what that means for their data. An individual who has parted with personal data is entitled, at the very least, to be informed when control over that data meaningfully changes. This is not a heavy burden on resolution applicants; it is the minimum that any informed consent architecture requires.

The hybrid model avoids the rigidity of both extremes. It preserves going-concern value by insulating continuity-essential processing from disruption. It protects Data Principal rights by requiring disclosure and fresh consent where processing purposes genuinely change. It allocates the burden of proof to the resolution applicant, who is best placed to demonstrate that a claimed use falls within the safe harbour and to explain the intended post-resolution uses of personal data. The law should be cautious of both extremes: assuming consent survives everything, or assuming it survives nothing.

V. CLAIMS, OVERRIDES AND LIMITS OF SECTION 31

Section 31 of the IBC provides that an approved resolution plan is binding on the corporate debtor and all insolvency stakeholders. The Supreme Court has given this provision considerable force, holding in *Essar Steel*[17] and *Ghanashyam Mishra*[18] that residual claims not reflected in the plan are extinguished. These decisions establish that the plan creates a comprehensive commercial settlement.

[17] Committee of Creditors of Essar Steel India Ltd. v. Satish Kumar Gupta, (2020) 8 SCC 531 (India)
[18] Ghanashyam Mishra & Sons Pvt. Ltd. v. Edelweiss Asset Reconstruction Co. Ltd., (2021) 9 SCC 657 (India)

An important distinction, however, separates the extinguishment of past monetary claims from the continuation of prospective statutory obligations. The cases establish that a creditor cannot seek payment of a pre-CIRP debt outside the plan. They do not establish that an enacted statute, particularly one enacted to give effect to a constitutional right ceases to apply to the corporate debtor or its successor controller upon plan approval.

Section 32A[19], which protects the corporate debtor by waiving certain criminal liabilities for pre-CIRP offences, is the one provision in the IBC that expressly addresses the intersection of insolvency relief with liability under other laws. It's very specificity suggests that where Parliament intends to carve out insolvency-related exceptions from the general law, it does so expressly. No equivalent carve-out exists for data protection obligations. The better interpretation is that ongoing compliance obligations under the DPDP Act including the obligation to process data only for consented or lawfully authorised purposes are not displaced by Section 31 approval. Although Section 238[20] gives the IBC overriding effect over inconsistent laws, not every parallel compliance obligation creates inconsistency. A requirement of notice, purpose-limited processing, or fresh consent for materially new uses does not inherently frustrate CIRP objectives. Harmonious construction remains preferable.

This conclusion is reinforced by the constitutional backdrop. Privacy is a fundamental right under Article 21[21], as recognised in Puttaswamy. The DPDP Act gives that right statutory expression in the commercial domain. It would require clear and unambiguous legislative language to hold that insolvency proceedings impliedly suspend fundamental rights protections for Data Principals and no such language exists in the IBC.

VI. COMPARATIVE GUIDANCE

A. United States: Toysmart and RadioShack

The United States encountered the intersection of insolvency and data protection in two widely noted cases. In *Toysmart* (2000)[22], the bankrupt online retailer proposed to sell its customer database as a standalone asset, notwithstanding a privacy policy that had expressly promised not to share user information with third parties. The Federal Trade Commission intervened,

[19] IBC § 32A
[20] IBC § 238.
[21] INDIA CONST. art. 21.
[22] In re Toysmart.com, LLC, No. 00-13995-CJK (Bankr. D. Mass. 2000)

contending that this constituted a deceptive trade practice. A settlement permitted sale only to an acquirer in the same line of business who assumed the original privacy commitments.

The principle that emerged was that privacy undertakings to users do not dissolve in bankruptcy because the data holder is insolvent.

In *RadioShack* (2015)[23], a proposed transfer of data relating to over 117 million customers to a buyer with different commercial intentions prompted intervention by multiple state attorneys general. The court imposed restrictions on the transfer, particularly for customers from states with restrictive data protection laws. Together, these cases illustrate that the identity of the acquirer and the intended use of personal data are legally material not merely the occurrence of a business transfer. They are persuasive guides for Indian courts and regulators, though they arise under different statutory frameworks.

These lessons are increasingly relevant in India. Insolvency practice is no longer confined to steel plants, infrastructure projects, or real-estate ventures. Proceedings now increasingly affect consumer-facing and technology-enabled enterprises. The insolvency of Jet Airways raised obvious questions regarding passenger records and loyalty databases, while the admission of AGS Transact Technologies to CIRP[24] demonstrates that transaction-intensive businesses may also enter resolution. As Indian insolvency increasingly engages with data-rich firms, comparative experience becomes more persuasive than remote.

B. GDPR and UK ICO Guidance

The General Data Protection Regulation provides the most developed framework for analysing controller changes in corporate restructurings. Under the current operating framework of GDPR, there is no automatic basis for the processing merely by virtue of the change of controller, the controller in succession must independently satisfy one of the grounds under Article 6[25]. In a case where processing is necessary for performance of a contract or dispersing the obligations of services, Article 6 (1) (b)[26] can be relied upon without obtaining the fresh consent. However, if the new controller intends to process data for purposes materially different

[23] · In re RadioShack Corp., No. 15-10197 (BLS) (Bankr. D. Del. 2015)
[24] NCLT Admits AGS Transact for Insolvency, The Economic Times (Aug. 22, 2025)
[25] Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 6, 2016 O.J. (L 119) 1 [hereinafter GDPR].
[26] GDPR art. 6(1)(b)

from the original, the purpose limitation principle in Article 5(1)(b)[27] requires either fresh consent or a structured compatibility assessment under Article 6(4)[28].

In the same manner, the UK ICO Guidance[29] for purchases and sales is also in line with these principles elaborated above. It generally emphasizes transparency and independent lawful basis assessment in business transfers, especially in cases of change in controller status, previous consents does not automatically transfers or carry forwards and that the purchasing entity must independently assess its lawful basis for each category of processing. These principles being followed in global jurisdictions are in consonance with the hybrid model proposed in this paper in and also offers practical guidance to Indian legislators for consideration.

VII. AN ILLUSTRATIVE EXAMPLE : A DIGITAL LENDER IN CIRP

Consider a non-banking financial company operating a mobile lending platform that enters CIRP following financial distress. The corporate debtor holds personal data for several hundred thousand borrowers: KYC documents, income records, bank account details, repayment histories, and device-level behavioural data. The data was collected under a privacy notice specifying use for credit assessment, loan disbursement, repayment monitoring, and regulatory compliance. A diversified financial services group acquires control through an approved resolution plan and subsequently contemplates three categories of use.

Category 1: Continuing loan servicing and recovery. This is processing necessary for performance of existing contracts and compliance with RBI and anti-money laundering regulations. It falls squarely within the continuity safe harbour and the legitimate-use provision of Section 7 of the DPDP Act. Prior consent survives. However, borrowers should be notified that a new entity now governs the lender.

Category 2: Cross-selling insurance and investment products. This purpose was not disclosed in the original privacy notice and does not arise from the contractual relationship the borrowers entered into. It is a materially new use. Fresh, specific consent is required before any such processing commences and borrowers must be able to decline without their loan

[27] GDPR art. 5(1)(b)
[28] GDPR art. 6(4)
[29] Information Commissioner's Office (UK), Buying or Selling a Business: Your Data Protection Obligations (2022)

servicing being affected.

Category 3: Transfer of behavioural data to a group analytics affiliate. This involves transferring data to a third party for a purpose entirely unrelated to the original lending relationship. It falls outside every ground in Section 7 of the DPDP Act and requires fresh, explicit consent. The issue would justify disclosure to, and potentially scrutiny by, the adjudicating authority or competent regulator.

This illustration shows that the relevant question is not binary. A single resolution transaction may encompass processing that legitimately continues under prior consent, processing that requires notice but not fresh consent, and processing that requires fresh consent in full. The legal framework must be calibrated accordingly.

VIII. PROPOSED INDIAN FRAMEWORK

The foregoing analysis suggests that neither absolute continuity nor universal re-consent is workable. A middle-path regulatory framework is preferable.

A. Mandatory Post-Resolution Notice

Within a specified period after NCLT approval under Section 31, the resolution applicant should be required to issue a notice to all Data Principals confirming: (i) the identity of the new controlling party; (ii) any material changes in processing purposes; (iii) details of any new third-party recipients; and (iv) how Data Principal rights may be exercised. This requirement could be operationalised through amendments to the IBBI's CIRP Regulations,[30] which already require disclosure of post-resolution management structure.

B. Continuity Safe Harbour

Processing that is strictly necessary for the performance of existing contracts, fulfilment of statutory obligations, or continuation of services in active use by Data Principals should be treated as covered by prior consent or the legitimate-use provisions of Section 7. The resolution applicant should bear the burden of demonstrating, upon request, that claimed processing falls within this safe harbour and involves no extension of purpose beyond what was originally

[30] Insolvency and Bankruptcy Board of India, Insolvency Resolution Process for Corporate Persons Regulations, 2016

disclosed.

C. Material Change Trigger

In cases where the resolution applicant proposes to process personal data in ways that significantly differ from the original purpose, it will be necessary to obtain fresh consent prior to the actual processing. Significant modifications encompass: (1) a shift in the principal identity or the owner of the Data Fiduciary; (2) an arrangement with alternative processors or affiliates; (3) the initiation of new processing objectives; and (4) any profiling or aggregation processes not previously disclosed.

D. Heightened Care for High-Risk Categories

Where the personal data in question related to high-risk category or sensitive information records such as financial records, health and medical data, biometrics or data relating to minors, additional safeguards should be put in place irrespective whether the processing qualifies for the safe harbour process. The movement of such data to other processors or affiliates must be based on newly acquired consent.

E. Regulator Coordination

The Insolvency and Bankruptcy Board of India and the Data Protection Board of India, once constituted under Section 18[31] of the DPDP Act should establish a coordination mechanism for CIRPs involving data-intensive enterprises. The RP should be required to notify the Data Protection Board upon commencement of proceedings affecting an enterprise holding personal data above a prescribed threshold. The Board should have standing to participate as an observer in such proceedings and to submit recommendations on data governance to the NCLT.

F. Resolution Plan Disclosure Requirements

IBBI Regulations should require resolution plans to expressly address data governance: the categories of personal data held; the resolution applicant's intended post-resolution uses; proposed transfers to third parties; the notice mechanism for Data Principals; and the security framework to be adopted. The NCLT should be empowered to impose conditions on plan

[31] · DPDP Act § 18

approval where data governance arrangements are found inadequate.

G. Decision Matrix: Post-Resolution Processing

Scenario	Fresh Notice Required?	Fresh Consent Required?
Continue servicing existing contracts (loans, subscriptions)	Yes	No — prior consent / § 7 legitimate use survives
Retention for statutory / regulatory compliance (KYC, AML)	Yes	No — statutory obligation under separate law
Cross-selling unrelated products or services	Yes	Yes — materially new purpose
Transfer to group affiliate for analytics or profiling	Yes	Yes — new recipient and incompatible purpose
New behavioural profiling or credit scoring for third parties	Yes	Yes — no original consent basis
Internal data security audits and access reviews	Yes	No — operational continuity and fiduciary duty

IX. ANALYSIS AND CONCLUSION

The resolution upon insolvency in a data-intensive enterprise through CIRP presents a structural question that neither the IBC or DPDP Act or any other special regulations that currently resolves: Whether the personal data held by the corporate debtor continues to be processed lawfully after a material change of control, and if so, on what terms.

The answer, on a careful reading of the relevant statutes, is that formal corporate continuity is

a necessary but not sufficient condition for the continuity of processing authority. What matters is whether those who now determine the purposes and means of processing are operating within the scope of the consent that Data Principals originally gave and whether those Data Principals have been told that anything has changed.

Section 31 of the IBC creates a binding and comprehensive settlement of insolvency claims. It does not, and should not be read to, extinguish the prospective statutory rights of Data Principals under a separate enactment giving effect to a constitutional right. The cases in which residual claims have been barred concern monetary obligations in the insolvency context, not ongoing compliance duties under data protection law.

The hybrid model proposed here offers a workable middle path. The continuity safe harbour preserves going-concern value and allows legitimate operational processing to continue without disruption. The material-change trigger protects Data Principals from having their data exploited for purposes they never contemplated by entities they never chose. The mandatory notice obligation ensures that individuals are not kept in the dark about who controls their data.

India has an opportunity, as it implements the DPDP Act and develops the IBC's operational practice, to adopt a principled and calibrated framework. The proposals in this article suggest a starting point. What is clear is that personal data cannot be treated as simply another asset that passes without restriction upon resolution. In a world expected to generate over 175 zettabytes of digital data annually, informational value is no longer peripheral to enterprise value. Many Indian data-intensive businesses also rely on globally distributed or cross-border storage infrastructure, making questions of post-resolution control and accountability even more significant. The individuals whose data underpins a resolution applicant's enterprise valuation have rights that persist after plan approval and the law should say so clearly.