III. FROM TARMAC TO TRUST: NAVIGATING A TURBULENCE-FREE FLIGHT PATH FOR DATA IN INSOLVENCY

Shaurya Kapoor[*]

ABSTRACT

The recent liquidations of SpiceJet and Jet Airways bring to the fore an overlooked legal issue that of what to do with passenger data when an airline is in corporate distress. Resolution professionals can and should maximise the value of the assets, including corporate data-driven ones, such as loyalty programs, passenger records, and transaction histories, under the Insolvency and Bankruptcy Code, 2016 (IBC). However, with the Digital Personal Data Protection Act, 2023 (DPDP Act), much greater safeguards have been placed on consent and the need not to have personal data spill over its intended purpose, and erasure, so the question arises whether such personal data can be commodified in insolvency without infringing individual rights. This paper looks critically at the conflict and crossing between the IBC and the DPDP Act. It takes a closer look at the Jet Airways CIRP and how data assets became the pivot of cross-border restructuring negotiations. Comparative learning experiences are also drawn from various jurisdictions. This paper will argue that the current Indian approach of taking a focused and regulated view of data as an asset, and a subject of insolvency, and securing privacy at the same time is necessary. It suggests specific exemptions under the DPDP Act in the context of insolvency and Standard Operating Procedures (SOPs) to be followed by the resolution professionals. A framework of this kind would match business efficacy with the constitutional promise of privacy in the context of both recovery by creditors and trust by consumers.

Keywords: Liquidation, CIRP, Standard Operations, Data and Asset.

[*] Shaurya Kapoor is a Third-year student of B.A.LL.B (Hons.) at the West Bengal National University of Juridical Sciences, Kolkata. The views stated in this paper are personal.

I. INTRODUCTION

India's aviation sector has been a witness to a lineup of airline insolvencies in recent times. From Kingfisher Airlines to Jet Airways, and also the more recent Go First Airlines.[1] This lineup exposes multiple legal gaps in how Insolvencies have been handled. Furthermore, the Insolvency Bankruptcy Code, 2016 **("IBC")** itself has been subject to six legislative enactments since its enactment in 2016, while the IBBI has also introduced over a hundred changes to the code.[2] While the broader question of whether IBC was enacted in haste persists, the aviation sector insolvencies point to a specific scenario where an oversight by the IBC can be pointed out. A neglected aspect of these airline insolvencies is the treatment of the vast amount of customer data held by these companies, including but not limited to names, contact details, travel histories, credit card information, etc. and sometimes even biometrics.[3]

---

[1] Financial Express, 'Jet Set Wait: The Airline's Liquidation Exposes the Shortcomings of India's Much-Vaunted Insolvency Resolution Process' (12 November 2024), <https://www.financialexpress.com/opinion/jet-set-wait-the-airlines-liquidation-exposes-the-shortcomings-of-indias-much-vaunted-insolvency-resolution-process/>; Rimjhim Singh, 'NCLT Approves Liquidation of Go First Airways Amid Insolvency Crisis' (*Business Standard*, 20 January 2025), <https://www.business-standard.com/companies/news/go-first-airways-liquidation-nclt-insolvency-bankruptcy-crisis-125012000326_1.html>.

[2] Sanjay Buch and Jay Zaveri, 'The Indian Insolvency Regime: Recent Amendments under the Insolvency and Bankruptcy Code 2016, (*International Bar Association)*<https://www.ibanet.org/article/3fb95409-8dc4-458e-be98-eafff085cc8c>.

[3] Statewatch, 'EU: European Commission to Propose EU PNR Travel Surveillance System, *Statewatch* (2011), archived at <https://web.archive.org/web/20120105132147/http://www.statewatch.org/news/2011/nov/eu-pnr-proposal.htm>.

When an airline goes into bankruptcy, this data could be sold, exposed, or even misused without any consent or knowledge of the passengers' consent. The Jet Airways case of 2019 is an illustration of the same, where passenger data was effectively treated as an asset in the resolution process.[4] Data is certainly a very valuable asset, generally, and for the purposes of insolvency proceedings for a company.[5] However, it is essential that its treatment does not come into conflict with data protection protocols.

The data privacy landscape in India has been fundamentally reshaped by the enactment of the DPDP Act.[6] Principles such as consent-based data processing, data minimization, and granting of data principles (individuals whose data is involved) the rights to withdraw consent and erasure of personal data when it is not required further for the specific purpose with which it was given are enshrined in the DPDP Act. There is also a mandated requirement of breach notification to the affected individuals as well as the authorities.[7] However, the DPDP Act is also silent on such specific scenarios, with the lack of any explicit exception or separate rules for the companies going under insolvency scenarios. This raises questions about the reconciliation of passenger data as an asset with the stringent consent and erasure requirements

---

[4] *State Bank of India & Ors v Consortium of Mr Murari Lal Jalan & Ors* (2024) SCC Online SC 3187.

[5] 'Data Privacy In Bankruptcy: The Consumer Privacy Ombudsman' (2025) 138 HLR 1451 <https://harvardlawreview.org/print/vol-138/data-privacy-in-bankruptcy-the-consumer-privacy-ombudsman/#:~:text=section%20363(b)(1,a%20debtor%E2%80%9D%20motions%20for%20it>.

[6] Digital Personal Data Protection Act No 22 of 2023 (India).

[7] Kirsten Doyle, 'Brace Yourselves: The Game-Changing Impact Of India's DPDP Act, 2023' (*Tripwire*, 16 June, 2025) <https://www.tripwire.com/state-of-security/brace-yourselves-game-changing-impact-indias-dpdp-act#:~:text=correct%2C%20and%C2%A0erase%C2%A0their%20personal%20data,a%20breach%20of%C2%A0personal%20data%20happen>.

under the DPDP Act. Does the Resolution Professional (hereinafter referred to as RP) have the right to retain and subsequently sell the passenger data (such as the loyalty program database in the Jet Airways case) as a part of the estate, and how do the data protection norms function in securing the rights of data deletion or protection, especially with the estate's value diminution consequently? Considering the same, this paper aims to pitch solutions that assist in harmonization of the goal of asset maximization under the IBC with the data protection protocols, specifically the Digital Personal Data Protection Act, 2023 (hereinafter referred to as the DPDP Act). It further examines the conundrum with the Jet Airways case as a key referral point.

A. Key Research Questions

1. Are there any conflicts between the IBC objective to maximise asset values and the DPDP Act requirements of consent, purpose limitation, and data subject rights in cases of insolvency over personal data, as in the case of an airline loyalty program?
2. How have Indian insolvency processes that include large amounts of personal data, such aviation sector, navigated this conflict between asset monetisation and data privacy in practice?
3. What operational and legal reforms can resolve such a conflict if it exists?

I. COMPARATIVE LEGAL AND REGULATORY APPROACHES: LITERATURE REVIEW

Personal data treatment in insolvency is an intensely contentious legal terrain, especially in digital economies, where assets consisting mainly of intangibles (such as data and code) can be a significant constituent of the value of an enterprise. International best practices are forged in different levels of coordination between insolvency regimes and privacy regimes, and every

surrounding jurisdiction can teach India both normative and practical lessons. In this section, prominent directions to this harmonization are outlined, and the relevance of these approaches to one another is highlighted.

A blueprint for the regulated commodification of data about insolvency proceedings exists in the United States. The landmark *FTC v. Toysmart.com* case illustrates the intervention of the Federal Trade Commission in blocking the sale of consumer data due to contravention of the company's own privacy policy by such a sale.[8] US has subsequently had reforms leading to the inclusion of privacy ombudsman safeguards within the U.S.C. section 363(b)(1) of the U.S. Bankruptcy Code,[9] while allowing selling of personal data when consistent with the debtor's previous privacy policy during bankruptcy. However, the idea of a privacy ombudsman, as well as section 363(b)(1), has been discussed at length in the Harvard Law Review paper titled *"Data Privacy in Bankruptcy: The Consumer Privacy Ombudsman."*[10] The paper contributes significantly to the debate of data privacy during insolvency, especially in the US context. It critically examines section 363(b)(1) and the privacy ombudsman requirement. The paper argues that despite being introduced as a means of injecting consumer-friendly checks into the mechanism of asset sales, in practice, the CPO mechanism has not been implemented as an effective oversight mechanism. Citing the examples of the *Borders Group* and *Celsius Network* cases,[11] the note points out the fact that CPOs generally lack institutional bargaining power, do not provide a veto, and are appointed in most cases at the discretion of the court, which exercises it not as a right, but rather as a discretionary power. Further, these ombudsman

[8] *FTC v Toysmart.com, LLC* (FTC File No. 002-3145, 21 July 2000) <http://ftc.gov/legal-library/browse/cases-proceedings/x000075-toysmartcom-llc-toysmartcom-inc>.
[9] Bankruptcy Abuse Prevention and Consumer Protection Act 2005, 11 USC § 363(b)(1).
[10] Data Privacy in Bankruptcy (n 6).
[11] *In re Borders Group Inc* (Bankr SDNY, No 11-10614, 14 September 2011); *In re Celsius Network LLC* (Bankr SDNY, No 22-10964, 4 January 2023).

reports are also largely advisory and the judges have continued to favour efficiency and maximization objectives.

This literature is especially instructive in terms of how a statutory framework can develop to accommodate data protection provisions in insolvency regimes, particularly where courts are encouraged to do so by regulators with an interest in protecting privacy such as the FTC. However, the paper does not discuss the interaction of the newer data protection regimes e.g. APPI in Japan,[12] or LGPD in Brazil,[13] with the insolvency proceedings, or the issues of localization requirements making cross-border data transfers during liquidation difficult. It also fails to capture a rising conflict between a growing number of sectoral data retention requirements (e.g., aviation, finance) and the broad concept of privacy in jurisdictions such as India and South Korea. Such a gap reinforces the importance of jurisdictions such as India developing both commercially feasible and rights-compliant hybrid models of insolvency-data privacy. This paper has left open the middle ground questions of comparative law, which are key to this paper: What should be the role of consent once the insolvency occurs? Who decides who will have continuing legitimacy of data use? And is insolvency law to govern over the principles of limitation of purpose that are embedded in the data protection laws?

Though more recently, in the U.S., the *RadioShack* bankruptcy case saw over 117 million customer records being offered for sale purposes, which led to a multi-state attorney general settlement restricting data use until prior consent was strictly respected.[14] However, this case simply indicates the lack

[12] Act on the Protection of Personal Information Act No 57 of 2003 (Japan).
[13] Lei Geral de Proteção de Dados Pessoais (General Law for the Protection of Personal Data) (Lei nº 13.709 de 14 de agosto de 2018) (Brazil).
[14] *In re RadioShack Corp* (Bankr D Del, No 15-10197, 2015) settlement details available at <https://www.sec.gov/Archives/edgar/data/96289/000119312515338728/d38755dex22.htm

of codified federal protection in the U.S, which allows ad hoc regulatory intervention only, and further indicates the weakness of consumer protection when privacy interests conflict with asset monetisation demands. Ultimately, this also highlights the issue of regulatory uncertainty in the U.S. with regard to this conundrum.

There are also anti-commodification inclined jurisdictions like that of the United Kingdom. Holding privacy as a right, similar to the legal status of privacy in India,[15] it becomes a compelling case to confront to evaluate if IBC asset monetization can even coexist. The *Thomas Cook* liquidation is a testament to this stance, where the Information Commissioner's Office warned publicly with regard to the sale or transfer of customer data without renewal of consent.[16] The General Data Protection Regulation (GDPR) of the European Union takes an even stricter stance by not recognizing data as a property of the enterprise itself.[17] Precisely, Article 5(1)(b) of the GDPR allows processing of personal data only for specified and lawful purposes.[18] Further, Article 6(1)(f) also allows data processing without consent for legitimate interests of the business, only if such interests are not overridden by any rights of the data subject.[19]

While privacy prioritization is commendable, Art. 5(1)(b) is devoid of the specificity needed for insolvency. The GDPR fails to strike a balance between commercial necessities of insolvency and the rights of data subjects, usually leaving resolution professionals with a stark dichotomous decision to make:

#:~:text=except%20as%20otherwise%20indicated%2c%20the,deadline%20to%20object%20to%20confirmation>.

[15] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 (SC).

[16] *In re Thomas Cook Group plc (in liquidation)* (Ch D, No CR-2019-006093, 25 September 2019).

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [2016] OJ L119/1.

[18] Regulation (EU) 2016/679 art 5(1)(b) 2016 OJ L119/36 (EU).

[19] Regulation (EU) 2016/679 art 6(1)(f) 2016 OJ L119/36 (EU).

delete data or face legal action. Although ethically sound, the strict anti-commodification framing can, by mistake, undermine the valuation of good assets, aggravate the collection of such assets by creditors, and deter restructuring. This lack of a tailored, insolvency-sensitive framework in the GDPR therefore bringing uncertainty, not clarity. Article 6(1)(f) also employs generic terms and has a dearth of specificity for insolvency. While it attempts to carve out some exceptions as a balancing act for legitimate interests, by subjecting them to the rights and freedoms of data subjects, it ends up going in circles.

With respect to many jurisdictions taking different paths in balancing data protection with the insolvency regimes, examining Japan's framework is essential, as it is an economy that commits to strong privacy policies as well as to its wide-ranging international business activities. The Act on the Protection of Personal Information (APPI) is a significant step towards balancing between user consent and fair use of commercial information,[20] an approach similar to what India should look towards. More importantly, APPI insists on a post-transfer use that must conform to the intended purposes or consent again. This provides a balance between the avoidance of freely commodifying data in insolvency to realize value. Reflecting an evolving data economy and the presence of remaining insolvency-data overlaps, APPI offers a convenient statutory benchmark in a potential future convergence of Indian laws.

The APPI does balance data commoditization and privacy, with Article 27(1)(ii) requiring prior consent for data transfers,[21] and Article 16(1) mandating the purpose limitation post-transfer.[22] This ensures that insolvency

[20] Act on the Protection of Personal Information Act 2003 (Japan) (n 12).
[21] Act on the Protection of Personal Information Act 2003 art 27(1)(ii) (Japan).
[22] Act on the Protection of Personal Information Act 2003 art 16(1) (Japan).

professionals cannot monetize data as they fancy. However, there is still a dearth of a proper oversight mechanism in place for such transfers. While cross-border data transfers are allowed under Article 28, it requires an "adequate" level of protection, and this list of adequacies is rather narrow, thereby largely limiting multinational insolvency resolutions.[23] However, the issue of enforcement uniformity is based on this limitation, compounded by the fact that Article 28 of APPI grants a relatively lenient opt-out regime in cross-border data transfers.[24] Whereas the law stipulates that there must be a provision of similar protection in the receiving country, it authorises such transfers even when there are no adequacy decisions issued, where the protection only rests on self-regulatory frameworks or on standard contractual clauses. This provides an opportunity to apply consent norms and post-transfer obligations inconsistently in insolvency, including voting inconsistency between before and after transfer, on a debt-by-debt basis where foreign resolution professionals or purchasers are involved. The lack of any required audits, or instantaneous regulatory oversight adds to the risk that personal information can be repurposed or monetised beyond the original purpose and negates the otherwise robust consent-based structure in APPI.

A similarly situated Global South jurisdiction that attempts a reconciliation of cross border data transfers and data privacy, as a developing digital economy, is Brazil. The General Data Protection Law (LGPD) in Brazil gives an extensive framework on cross-border data transfers.[25] Article 33 of the LGPD provides that international transfer can only be enabled under one of the following mechanisms: adequacy decisions, ANPD-approved Standard

[23] Act on the Protection of Personal Information Act 2003 art.28 (Japan).
[24] Andrew Clearwater, 'Japan's Amended APPI Comes into Effect: These APPI Amendments Include Data Breach Reporting, Stricter Data Transfers, and Increased Data Access Rights' (*OneTrust*, 1 April 2022) <https://www.onetrust.com/blog/japans-amended-appi-comes-into-effect/>.
[25] General Law for the Protection of Personal Data (Brazil) (n 14).

Contractual Clauses (SCCs), Binding Corporate Rules (BCRs) or specifically-authorised specific contractual clauses.[26] Resolution CD/ANPD No. 19/2024, of the National Data Protection Authority (ANPD) in August 2024, has outlined details of SCCs, equivalence assessment, and transparency requirements.[27] The SCCs will have to be used verbatim, and a set of transparency requirements, including disclosures on websites and enabling data subjects to access the text of comparable clauses within 15 days, will follow. The Brazilian model balances privacy with commercial flexibility, similar to the APPI, but with structured enforcement safeguards.

Despite its structured approach, the Brazilian system exposes weaknesses in terms of its enforcement and timing, especially when it involves insolvency situations. So far, ANPD has not made any adequacy decisions, and this has necessitated the use of SCCs as the only possible ready-made alternative. Approval of BCRs or clauses takes time and has not been definitively decided, leading to a legal bottleneck.[28] In cross-border insolvency situations, this may cause an incoherent application of privacy standards. Buyers may act on unverified clauses or have to wait to obtain information that is crucial to asset valuation. Moreover, the transparency requirements provided in Brazil cannot ensure real-time control; no regulatory audits or quick enforcement measures can be applied to eliminate the possibility of insolvent entities monetizing the personal data under poorly enforced safeguards. Lastly, the inflexibility of SCCs, although privacy-preserving, can prohibit effective restructurings, as

---

[26] General Law for the Protection of Personal Data, arts 33–36 (Brazil); Fernando Bousso and Matheus Kasputis, 'Brazil's New Regulation on International Data Transfers' (*IAPP*, 4 September 2024) <https://iapp.org/news/a/brazil-s-new-regulation-on-international-data-transfers>.

[27] ANPD Resolution CD/ANPD No 19/2024 (Brazil); Trade.gov, 'Brazil's New Rules on International Data Transfers' (12 August 2025) <https://www.trade.gov/market-intelligence/brazils-new-rules-international-data-transfers>.

[28] Renata Neeser, 'Brazilian SCCs Only Viable Mechanism Now' (*JD Supra*, 12 August 2025)<https://www.jdsupra.com/legalnews/brazil-standard-contractual-clauses-8491471/>.

well as disincentivize foreign bidders, unused to the hard formatting under Brazil.

Although the privacy protection of Japan APPI and Brazil LGPD contains compelling cross-border privacy protections, neither framework resolves the specific exigency of insolvency proceedings, where the transfers of data might be time-sensitive and value-based. In the lack of specific insolvency-related statutory regulation and live regulation inspection, the voluntary nature of insolvency rules and regulations threatens to derail their voluntary mechanisms by permitting data to be commercialised or moved without any sufficient procedural discernment, thus affecting both debtors and creditors to the possibilities of legal obscurity.

Indian research and legislation on the other hand, is scant in the interplay between data protection and insolvency despite the burgeoning interest in the field globally. This gap in passenger data treatment after insolvency, especially in the aviation industry, has been noted in one such commentary in *Legal500*,[29] which calls out lack of specific protection against the monetization of confidential customer information by acquirers or resolution professionals as outlined in the DPDP Act, 2023.[30]

The other contribution of particular interest is by Adam Feibelman and Renuka Sane, who support a maximalist treatment of the information in an insolvency system, but their inferential contribution is to institutional transparency and efficiency of information rather than privacy per se.[31]

---

[29] Agrud Partners, 'Airline Insolvency in India: Legal Gaps in Lessors' Rights and Passenger Data Protection (*Legal500*, 10 June 2025)<https://www.legal500.com/developments/thought-leadership/airline-insolvency-in-india-legal-gaps-in-lessors-rights-and-passenger-data-protection>.

[30] Digital Personal Data Protection Act 2023 (India).

[31] Adam Feibelman and Renuka Sane, 'A Maximalist Approach to Data from India's New Insolvency and Bankruptcy System' (Tulane Public Law Research Paper No 19-4, 28 December 2018) <https://ssrn.com/abstract=3311195> or <http://dx.doi.org/10.2139/ssrn.3311195>.

Although these discussions are useful, significant gaps can be observed. The literature on formulating or collecting macro-level information on the reformation or bankruptcy administration does much of the existing literature, failing to spotlight the privacy threats and legal tangles arising when the personal data eventually falls into the estate of the debtor. Operational and doctrinal analyses are absent. How the consent and erasure requirements in the DPDP Act and RP requirements under the IBC are at loggerheads, or what regulatory regimes can lawfully potentially guide cross-border data transfers as part of a resolution.

Therefore, even as these jurisdictions and commentaries present diverse approaches to regulatory ideas, their failure to harmonise insolvency-specific needs with data protection requirements reveals a sharp necessity in an equilibrated hybrid model, which the paper now goes on to develop in the Indian context. This further underscores the essential contribution that this paper seeks to make by extending the conversation to fill the void presented above by proposing procedural and legislative reforms for the reconciliation of data protection and insolvency. If India effectively acts on the same towards its addressal, it could lead to a potential framework for various digital economies to refer to.

II. ANALYSING THE CONFLICT BETWEEN THE IBC, 2016 AND THE DPDP ACT, 2023

A. Legal Treatment of Data as an Asset in the Indian Insolvency Landscape

The Supreme Court of India in *Justice K.S. Puttaswamy v. In the Union of India (2017)* case judgment, the right to privacy was established as a

fundamental right under Article 21 of the Constitution.[32] Another important aspect of this ruling was the establishment of informational privacy, which is the right to control the circulation and use of personal data by people. The Court reiterated the role of individuals in the data economy not as passive data subjects but active data principals, with an ability to make decisions over their personal information. Critically, firms that receive such information are referred to as data fiduciaries who are merely custodians of the data but not the owners of the data.

However, the customer data and, in particular, data aggregated into databases remain a potentially monetized asset to commercial and insolvency law. Airlines, e-commerce companies, and technology companies use data as capital. The IBC 2016 has an expansive definition of assets that form a part of the debtor's estate and explicitly includes intangible assets in the same.[33] A key point of reference, which will also be further elaborated upon in this paper, is the case of Jet Airways, one of whose most treasured property assets was its ownership stake with Jet Privilege Pvt. Ltd. (JPPL), the operator of its frequent flyer programme.[34] JPPL also had the personal and behavioural data of more than 9 million passengers under management. Using nearly all this data, valuations estimated the company to be worth more than 7,000 crore.[35] This customer base met the fancy of bidders, including global investors.

India's Digital Personal Data Protection Act, 2023 (DPDP Act),[36] which frames a modern consent-based data governance framework, but does not specifically address data governance in insolvency situations. It puts into

[32] *Puttaswamy* (n 16).
[33] Insolvency and Bankruptcy Code No. 31 of 2016 § 18(f)(iv) (India).
[34] Gopika Gopakumar and Rhik Kundu, 'Jet Airways' Stake in Frequent Flyer Scheme Key for Potential Bidders' (*Mint*, 21 July 2019) <https://www.livemint.com/companies/news/jet-airways-stake-in-frequent-flyer-scheme-key-for-potential-bidders-1563730990896.html>.
[35] ibid.
[36] Digital Personal Data Protection Act 2023 (India).

writing the fundamental principles that include purpose limitation, informed consent, data minimization, and right to erasure. Section 8(7) states that a person must erase the personal data when the purpose is reached, or when the individual has withdrawn his or her consent, unless it needs to be held in order to comply with any law.[37] Also, the DPDP Act in Section 16(1) enacts a localisation requirement, which obliges the storage of significant classes of personal data in India, providing one more layer of compliance by cross-border bidders in insolvency proceedings.[38]

However, the Insolvency resolution is not considered as a legitimate basis to retain the data, and similarly, the Act does not create exemptions for resolution professionals (RPs) or liquidators who work under the IBC, 2016. This adds legal uncertainty because RPs are mandated under Sections 25 and 29 of the IBC to maintain and maximize the value of the assets of the corporate debtor, including datasets,[39] but transferring or otherwise monetising such data that is not required by the IBC without a renewed consent or statutory basis may violate the DPDP Act. This brings a fundamental tension, while data protection law favours dignity and consent, insolvency law favours value maximization.

B. Case Study: Illustrating the IBC and DPDP Conflict via the Jet Airways Insolvency

Jet Airways, which was one of the largest airways belonging to the private sector of India, closed down in April 2019 on account of financial turmoil. In June 2019, the airline entered the Corporate Insolvency Resolution Process

[37] Digital Personal Data Protection Act 2023 s 8(7) (India).
[38] Digital Personal Data Protection Act 2023 s 16(1) (India).
[39] Digital Personal Data Protection Act 2023 SS 25(C), 29(2) (India).

(CIRP) under the IBC 2016, at the request of the creditors.[40] The recovery of such a company was left to the Resolution Professional (RP) to identify a resolution applicant or to drive the company into liquidation. During the insolvency proceedings, Jet Airways had only a few tangible assets; most of the aircraft were on lease, and there was no real estate. However, there is one important intangible asset that caught the attention, a 49.9 percent stake in JetPrivilege Pvt. Ltd. (JPPL), which is involved in managing loyalty programs. The rest, or 50.1 percent of JPPL, was owned by Etihad Airways. When Jet collapsed, JPPL kept functioning under the shelter of Etihad and re-branded to the name of "InterMiles" in 2020.[41]

By the middle of 2019, JetPrivilege had a database with more than 9 million frequent flyer members. The profile of these members contained names, travel history, meal preferences, passport information, and other sensitive personal information, which could be a very valuable resource to any bidding entity that wants to restore or use the Jet brand name.[42] Nevertheless, JPPL was a distinct corporate entity, which meant that all the RP could transfer was Jet 49.9 per cent ownership in JPPL, not the data itself. Notwithstanding this shortcoming, the worth of the data played a big role in attracting potential bidders in the case of JPPL, which has been estimated to be 7,300 crore (approximately 1.1 billion USD) by the industry watchers.[43]

This raises two key legal issues:

---

[40] Koustav Das, 'Jet Airways Retail Shareholders Stare at Total Loss after Liquidation Order: Report' *India Today* (7 November 2024) <https://www.livemint.com/companies/news/jet-airways-stake-in-frequent-flyer-scheme-key-for-potential-bidders-1563730990896.html>.
[41] ET Bureau, 'Jet Privilege Goes for Brand Revamp; to Be Known as 'InterMiles'' *Economic Times* (14 November 2019) <https://www.economictimes.indiatimes.com/industry/transportation/airlines-/-aviation/jet-privilege-goes-for-brand-revamp-to-be-known-as-intermiles/articleshow/72053969.cms>.
[42] Gopika Gopakumar and Rhik Kundu (n 35).
[43] ibid.; Agrud Partners, 'Airline Insolvency in India: Legal Gaps in Lessors' Rights and Passenger Data Protection' (n 30).

1. Firstly, Jet did not own the passenger data and was merely an equity holder in the entity owning the data.

2. Secondly, even if a sale occurred, could the transfer of customer data without their informed consent be legally done as a part of Jet's insolvency estate?

While in Jet's case, a question of data ownership arises, the same would not arise in a case where a company directly owns data, which is the focus of this paper. There was no general data protection law in India during the period when no Personal Data Protection Bill, 2019 (then pending) or the current Digital Personal Data Protection Act, 2023 (DPDP Act) were applicable. This provision of law would leave privacy rights vulnerable to the contractual privacy policy of JPPL and its own ethical norms. Etihad continued to retain operational control of InterMiles, and the loyalty program was continued for members.[44] This arguably may mitigate some immediate privacy risks. The situation could vastly differ if Jet's JPPL stake passed to another organization or a competing airline. Hence, the fundamental legal ambiguity regarding the sale of passenger data without informed and active consent continued to be unaddressed.

If the entire Jet Airways insolvency saga is to be viewed from the perspective of the DPDP Act, 2023, serious legal crossroads would arise. Firstly, the Act requires erasure of personal data by data fiduciaries post fulfilment of the purpose of withdrawal of consent, unless retention is legally mandated.[45] In fact, the new Draft Digital Personal Data Protection Rules, 2025, suggest a three-year inactivity threshold for significant data fiduciaries

[44] ibid.
[45] Digital Personal Data Protection Act 2023 s 8(7) (India).

(SDFs), post which it requires a mandatory data deletion.[46] Such a threshold would be easily crossed in the Jet Airways case.

A new data fiduciary would further require fresh consent and notice before processing the acquired data,[47] and the DPDP also requires data processing only for the originally specified purpose.[48] Therefore, any transfer or revival of any kind for these loyalty programs would require proper reassessment of purpose and fresh opt-ins. Moreover, the DPDP Act, 2023, though it allows cross-border data transfer, follows a negative listing approach whereby the Central Government can bar certain jurisdictions from such a transfer.[49]

The DPDP Rules, 2025, further propose a white-listing type model, including empowering the Central Government to place conditions on access to Indian personal data for certain foreign states and localization-specific data classes for SDFs.[50] This practically makes cross-border resolutions legally challenging and cumbersome to operate, as data was collected under a currently defunct fiduciary's policies and terms and conditions. Especially, if the third party wishes to use it for a different purpose, such as targeted marketing or an alternate scheme. This could, in fact, draw penalties under the DPDP for unlawful processing, up to rupees two hundred crores.[51] Unlike Article 6(1)(f) of the GDPR, the Indian law also lacks a "legitimate interest"

[46] Ministry of Electronics and Information Technology, Draft Digital Personal Data Protection Rules, 2025, rule 7(2) (India).
[47] Digital Personal Data Protection Act 2023 s 16(1) (India).
[48] Digital Personal Data Protection Act 2023 s 5 (India).
[49] Taxmann,'Cross-Border Data Transfers under the DPDP Act 2023' (last updated 4 May 2025) <https://www.taxmann.com/post/blog/cross-border-data-transfers-under-the-dpdp-act/>.
[50] Trilegal, 'The Draft Digital Personal Data Protection Rules, 2025 – Operationalising India's Data Protection Law' (3 January 2025) <https://trilegal.com/dataprotection/the-draft-digital-personal-data-protection-rules-2025-operationalising-indias-data-protection-law/>.
[51] Digital Personal Data Protection Act 2023 s 33 (India).

basis for personal data processing based on a business justification without consent.[52]

Furthermore, DPDP allows data principal to withdraw consent for their data in its entirety, and such a request during the insolvency process would directly conflict with the IRP's/RP's duty to take control and custody of the asset and protect and preserve the same.[53] If a moratorium were to be further imposed under Section 14,[54] any deletion of data by the data principals could arguably cause these estate assets to be disposed of in an unauthorised manner. This could also conflict with the value maximization goal of the IBC as if data as an asset becomes susceptible to deletion based on the data principal's consent, its value gets jeopardized.

On the data protection front, while the IBC states that Insolvency Professionals (IPs) must follow "reasonable care and diligence" in their professional conduct,[55] no specific protocols exist with regard to the handling of personal data. Moreover, the DPDP itself also lacks any exceptions or safe harbour for RPs and the risk of civil as well as criminal liability remains active.[56]

The Jet Priviledge case, hence, serves as a caution for any data-based insolvencies in the future, pointing to a requirement of integration between data protection laws and the IBC, without which these frameworks will continue to be at a crossroads, and the conundrum will continue. Such a regulatory gap contributes to variable practice and detracts predictability of outcomes to the bidders, creditors, as well as data principles.

---

[52] Regulation 2016/679, art 6(1)(f) (n 20).
[53] Insolvency and Bankruptcy Code 2016 ss 18(f) 25(1) 25(2)(c) (India).
[54] Insolvency and Bankruptcy Code 2016 s 14 (India).
[55] Insolvency and Bankruptcy Code 2016 s 208(2)(a) (India).
[56] Digital Personal Data Protection Act 2023 ss 33–34 (India).

IV. RECONCILIATION OF THE IBC, 2016, AND THE DPDP, 2023: TOWARDS A HARMONIZED FRAMEWORK

To ensure that the insolvency regime in India does not come into conflict with the emerging data protection landscape in the country, there is a need to formulate both legal and practical changes. There are a few conceptual and practical challenges where the IBC and the DPDP intersect, as previously discussed. Accommodating both the commercialisation of data assets and the privacy concerns of individuals poses a dual challenge, namely, how to allow resolution professionals (RPs) to take advantage of the commercial value of data assets without infringing the privacy rights of individuals. It demands a two-pronged solution: Specific amendments to the IBC and DPDP Act, and operative procedures to be followed by insolvency professionals, in the form of standard operating procedures (SOPs).

A. Recognition of Data as a Regulated Asset under the IBC

The legal recognition of personal data as one of the constituents of the insolvency estate and the recognised regulatory nature of personal data shall be the first reform agenda. The interests of personal data are now covered by the term of assets according to IBC, yet it is not defined and does not imply a particular inclusion. Nevertheless, in a digital economy, a database of customer information is typically a valuable resource for companies.[57] To make such assets subject to the insolvency resolution, the phrase "assets" should be supplemented in either Section 18(f) (giving the interim resolution professional control of assets of the corporate debtor) or Section 36(3) (defining the liquidation estate), to clarify that the term extends to databases,

[57] OECD, *The Value of Data in Digital-Based Business Models: Measurement and Economic Policy Implications* (2020).

digital repositories and personal data of the debtor.[58] However, only insofar as such data is being processed in line with the applicable data protection law.

B. Carving Insolvency-Specific Exemptions under the DPDP Act

Although the DPDP Act does provide that personal data may be processed without the consent of the owner when it is required by law,[59] this broad delineation does not necessarily provide sufficient guidance in insolvency legislation. To ensure this, a new provision under DPDP rule-making power authority would provide that data processing may be carried out by an RP under the IBC and will be deemed lawful under Section 7(b) of the Act in case it is strictly necessary in the context of insolvency including, but not limited to resolution, sale as a going concern,[60] or liquidation.

In a situation where the requirements of the IBC and the DPDP Act come into conflict, e.g., when a data principal's right to erasure under the DPDP Act is exercised,[61] but the data sought to be deleted is considered vital to continued insolvency resolution efforts, then a limited and specific exemption should be provided. This clause must clearly make it clear that during the short period that the Corporate Insolvency Resolution Process (CIRP) or liquidation proceedings may be in progress, the mandates of resolution professionals under the IBC will be accepted over any conflicting mandate laid out by the DPDP Act. For reference, CIRP may need customer transactional data or past consent logs in assessing proposals by bidders or in determining claims. Allowing deletion at this point would serve to provide a frustration to the

---

[58] Insolvency and Bankruptcy Code 2016 ss 18(f) 36(3) (India).
[59] Digital Personal Data Protection Act 2023 s 7(b) (India).
[60] IBCLAW, 'Going Concern Sale during the Liquidation Process under Insolvency and Bankruptcy Code, 2016 (IBC)' (*IBC Law*, 25 May 2019) <https://ibclaw.in/going-concern-sale-during-the-liquidation-process-under-insolvency-and-bankruptcy-code-2016-ibc/>.
[61] Digital Personal Data Protection Act 2023 s 12(3) (India).

resolution objective in Section 31 of the IBC.[62] But to preclude the vast derogation of privacy in this override, it must be strictly limited. It must only be applied to data that can clearly be shown to be required for insolvency-related purposes, and must automatically expire with the adoption of a resolution plan or entry of liquidation. Standard DPDP obligations, e.g., data minimisation, purpose limitation, should be reverted to after the appropriations, and continued use or transfer of personal data should either be consent-based or within one of the few statutory reasons under Section 7 of the DPDP Act.[63] This framework would not bring the IBC to undertake a commercial purpose at the expense of the essence of the privacy protections offered in data law.

The DPDP framework allows the Central Government to notify sector-specific rules to deal with privacy considerations that may be issues related to various context sensitivities.[64] In consideration of this, a specific provision, which can be referred to as *"Processing of Personal Data during Insolvency or Restructuring"* should be developed. The first rule should give the Resolution Professional (RP) the statutory status of a data fiduciary in a Corporate Insolvency Resolution Process (CIRP), making the RP subject to all the provisions of a data fiduciary under the DPDP Act, including the information purpose limitation, data minimisation, and lawful processing requirements in Section 8 of the DPDP Act.[65]

---

[62] Insolvency and Bankruptcy Code 2016 s 31 (India).
[63] Digital Personal Data Protection Act 2023 s 7 (India).
[64] Digital Personal Data Protection Act 2023 s 11(3) (India); Shivalik Chandan and Others, 'India: Examining the Digital Personal Data Protection Act as Government Publishes Draft Rules Ahead of Implementation' (*Global Investigations Review*, 31 July 2025) (noting that sector-specific laws in areas such as banking, insurance, healthcare, and telecom "continue to apply, provided they do not conflict with the provisions of the DPDPA or are expressly repealed.")<https://globalinvestigationsreview.com/guide/the-guide-cyber-investigations/fourth-edition/article/india-examining-the-digital-personal-data-protection-act-government-publishes-draft-rules-ahead-of-implementation>.
[65] Digital Personal Data Protection Act 2023 s 8 (India).

Furthermore, to provide transparency in insolvency regarding data processing, the rule must specifically require the RP to provide notice to all data principals that (a) insolvency has occurred; and (b) their personal data, which had at that point been gathered and processed by the corporate debtor, will thereafter be handled differently. This notice should describe how the information will be used: retained only for post-resolution activities, handed over to a successful resolution applicant, or anonymized and removed after CIRP. This reflects the obligations of transparency provisions under regimes such as GDPR,[66] where a data subject must be informed about material changes in the context of control and processing.

Also, any resolution applicant or acquirer that wants to access the data assets of the corporate debtor, such as its customer list, usage pattern, or loyalty database, should be mandated to either (a) use the same data solely for the original intended purpose, or (b) obtain the express and individual consent of the data principals in case it wants to use the data in a new purpose. Such a requirement upholds the principle of limiting purposes of use under Section 8(2) c of the DPDP Act,[67] and discourages lapses in using personal data as a commodity to make a quick profit without due process.

C. SOPs for Resolution Professionals

Apart from legislative amendments, it is advised that the Insolvency and Bankruptcy Board of India (IBBI) and the Data Protection Board (DPB) collaborate on elaborating a comprehensive Standard Operating Procedure (SOP) that RPs follow when handling personal data in the course of insolvency proceedings. Regulatory SOPs have been a longstanding regulatory practice; for instance, the Reserve Bank of India (RBI) had issued a Master Direction

[66] Regulation 2016/679, arts 13, 14 (n 18).
[67] Digital Personal Data Protection Act 2023 s 8 (2)(c) (India).

on Digital Payment Security Controls, which included SOPs for customer data management, upholding encryption, and mandated a secure transfer if a business is discontinued in the event of shutdown or mergers.[68] Such a model should be created for the insolvency domain to fill the operational void between the IBC and DPDP regimes with a gradual data governance environment.

The SOP must start with the obligatory data mapping, when RP will be required to provide a comprehensive list of all the personal data possessed by the corporate debtor. This is spread across customer names, contact information, payment and travel history, browsing history (where applicable), loyalty program data, and related metadata. The RP should further analyse the privacy policy of the debtor to gauge the legality of pre-CIRP gathering of the data, especially clauses dealing with transfers of data during mergers/ restructuring, with the help of which limited application of these clauses post-CIRP can be initiated. The RP should be obliged to introduce secure access and storage controls after this. Under section 8(5) of the DPDP Act, reasonable security measures against breaches are required to be taken.[69] To that end, the SOP must mandate such items as encryption at rest, access logging, multi-factor authentication, and third-party security audits. Where customers revoke their consent or request erasure of the data, the RP can invoke the exemption in Section 7(b),[70] which is based on legal obligations to retain such data where that is necessary to preserve the estate. An example is that deleting loyalty transaction histories can drive down the value of a monetised frequent flyer programme in CIRP. The RP can also initiate NCLT permission to defer loss

[68] Reserve Bank of India, *Master Direction on Digital Payment Security Controls* § 7.2.2 (18 February 2021) (mandating business continuity and customer data safeguards during business transitions or shutdowns).
[69] Digital Personal Data Protection Act 2023 s 8 (5) (India).
[70] *id.* s 7(b) ("processing necessary for compliance with any law for the time being in force").

of deletion obligations as part of CIRP on the basis of commercial need and burden of compliance.

To maintain transparency, it is advisable that the SOP compel the RP to issue notices in public domain, including via email, the firm's webpage, or through publication on stock exchanges, to inform data principals that (a) the corporate debtor is in a situation of insolvency, (b) the RP is the trustee in place, and (c) that the obligations and restrictions regulating processing operations, as prescribed by the law, will be observed to the letter during CIRP.

In a case where resolution applicants request disclosure of data, layering disclosure should be suggested in the SOP. Preliminary figures must be anonymised or aggregated. When granular or identifiable data is required, a Non-Disclosure Agreement (NDA) and a Data Processing Agreement (DPA) will be signed. Such agreements must oblige the applicant to erase the data in the case of an unsuccessful bid and utilize it only according to the evaluation purpose.

Once a resolution plan is passed, the new data fiduciary is the winning applicant. The SOP should also instruct the RP to proceed with a structured handover, including providing consent logs, any outstanding data subject requests, reports of previous breaches, and any other obligations that are assumed under the privacy policy. The new fiduciary is obliged either to keep utilizing the information on the same basis as above or to seek new informed consent, a policy captured in the purpose limitation principle under the DPDP Act.[71]

In cases of liquidation, the SOP would have to differentiate between a situation where personal data needs destruction and where such data is to be

[71] *id.* s 6(2) (data can only be used for specified, lawful purposes and must be deleted when no longer necessary).

sold as assets. In the event that the liquidator intends to monetise personal data, such as the customer lists, loyalty program logs, or usage analytics, as a part of an asset sale, the SOP should encompass high procedural safeguards. The data should only be sold to a data fiduciary as defined by the DPDP Act,[72] who is willing to abide by its duties (considering the parallelly suggested amendments and additions in the DPDP Act). Second, the sale of the data must be within the scope of the initial collection purpose for which the data was collected and informed to the data principals, or it must be the subject of new, informed consent among the data principals. The requirement of proper notices, as previously delineated should be required.

In case a buyer is not found or the data is no longer required with a legal or business aspect, it should be deleted or anonymised in accordance with industry standards, i.e., DoD 5220.22-M or NIST 800-88 programs.[73] A final report of compliance and a public notice are to be issued that proves data disposal and closure of fiduciary obligations.

D. Balancing Cross-Border Transfer Restrictions

In instances such as JetAirways, cross-border sharing is contentious, where proceedings in the Netherlands were conducted simultaneously with the Indian CIRP.[74] DPDP Act places a limit on data transfers to jurisdictions negatively listed by the government of India.[75] The Draft DPDP Rules, 2025, provide additional constraints as the Centre may impose other restrictions, such as access by foreign States.[76]

---

[72] Digital Personal Data Protection Act 2023 s 3 (d) (India).
[73] National Institute of Standards & Technology, *Guidelines for Media Sanitization*, Special Publ'n 800-88, Rev 1 (December 2014).
[74] Olivia Nahak, 'The Jet Airways Case: Addressing India's Cross-Border Insolvency Inadequacies' (*IBC Laws*, 5 August 2025) <https://ibclaw.in/the-jet-airways-case-addressing-indias-cross-border-insolvency-inadequacies-by-olivia-nahak/>.
[75] Taxmann, 'Cross-Border Data Transfers under the DPDP Act 2023' (n 50).
[76] Trilegal, 'The Draft Digital Personal Data Protection Rules, 2025' (n 51).

For such scenarios, the Rules need to be amended to grant a foreign bidder a carve-out as an opportunity to perform due diligence. Transfer in the case of contractual adherence by the foreign party to Indian standards, and submission to the Indian jurisdiction for dispute resolution, though the country that might be blacklisted, could be admitted.

V. CONCLUSION

The business insolvency of companies dealing directly with the people, such as Jet Airways, highlights one such key policy gap in law, i.e., the regulation of personal data, which can be paramount in terms of value and should be more firmly entrenched within the insolvency regime. The DPDP Act, 2023, is right in focusing on personal data privacy, whereas the IBC 2016 is based on the idea of maximisation of asset value to creditors. These goals do not have to be contradictory. A structured integration is not only feasible but necessary, as was discussed in this paper.

This paper demonstrates that under the current state of law, resolution professionals are placed in an untenable position; expected to maximise value (including data) under the IBC, but also potentially endangering consent and erasure obligations under the DPDP. This problem is compounded even in cross-border cases, where data localisation and limitations on the transfer of data may impede any restructuring involving bidders in other jurisdictions. By analysing the legislative gaps in detail, through comparative studies surrounding the U.S., EU, Japan, Brazil, and the Indian context, this paper has proposed a balanced legal and procedural framework. Both regimes can be aligned by recognising personal data as a regulated asset, with the insolvency professionals being given clear SOPs and fiduciary responsibilities, and carving out two narrow, time-limited exemptions under DPDP.

There needs to be, however, not a trade-off decision between privacy and a business rescue, but an integration of the two. Information privacy is vital to the respectability of a resolution plan, and in a digital economy, a resolution plan cannot afford to lose that quality. Jet Airways must not only be regarded as a learning experience, but also a legislative turning point- one that will lead India to mature insolvency laws that can accommodate the digital future of our country.