PRIVACY OF INSOLVENCY PRACTITIONERS: COMPARATIVE ANALYSIS OF UK (GDPR) AND INDIA (DPDP ACT, 2023)

Ishan Mankotia[1] & Mr Sheheen Marakkar[2]

ABSTRACT

Therefore, in this paper, a comparative legal analysis will be performed between the privacy rights and responsibilities of insolvency practitioners (IPs) in India under the Insolvency and Bankruptcy Code, 2016 (IBC) and Digital Personal Data Protection Act, 2023 (DPDP Act) against the Insolvency Act 1986 and the maintained GDPR of the UK. With digital assets increasingly taking over the current Corporate Insolvency Resolution Processes (CIRP), IPs have access to extensive personal datasets - creditor PAN/Aadhaar information, employee databases, customer databases, etc. - to verify claims, value them, and decide upon resolutions, tensions emerge between the disclosure requirements of IBC (Sections 15, 18, 25) and the fiduciary obligations of DPDP (Sections 4-12), which are fiduciary in nature.

The review shows that DPDP, with its inflexible use of legitimate uses, lack of the sectoral guidance and strong minimization, conflicts with the IBC transparency requirement, as opposed to GDPR whose lawful bases are flexible (legal obligation, a legitimate interest), ICO advisories on insolvency and judicial clarity (Southern Pacific, 2014). UK IPs have strong rights to refuse DSARs/erasure, disclose data to creditor committees and rely on forensic audit, cushioned by tests of proportionality, whereas Indian Resolution Professionals are helplessly exposed to compliance paralysis, data breach and delay in operations under vague exemption.

The major obstacles are consent infeasibility, conflicts between confidentiality and transparency, and excessive burdens of small IPs. The proponents of comparative insight recommend moderated reforms: joint IBBI-DPBI rules that affirm insolvency exemptions, compulsory DPIA, anonymous disclosure, and RP training to align frameworks without undermining the recovery of creditors.

This paper talks about comparison between the privacy rights and

[1] Mr Ishan Mankotia, Student, CHRIST (DEEMED TO BE UNIVERSITY), Pune Lavasa Campus
[2] Mr Sheheen Marakkar, Assistant Professor**,** CHRIST (DEEMED TO BE UNIVERSITY), Pune Lavasa Campus

responsibilities of insolvency practitioners (IPs) in India under the Insolvency and Bankruptcy Code, 2016 (IBC) and Digital Personal Data Protection Act, 2023 (DPDP Act) against the Insolvency Act 1986 and the maintained GDPR of the UK.

Keywords: Privacy, Insolvency, Data, Protection, Creditors

Introduction

The Insolvency and Bankruptcy Code, 2016 (IBC) of India completely transformed the process of corporate insolvency by introducing a time-limited Corporate Insolvency Resolution Process (CIRP), in contrast to the Insolvency Act 1986 of the UK which has more flexible ways of salvaging business such as administration and liquidation. The related data privacy has taken on a leading role in both jurisdictions in the insolvency proceedings, where practitioners regularly access large volumes of sensitive personal data, such as employee salary records, creditor PAN and Aadhaar information, customer transaction histories, and proprietary databases, which comprise the most critical intangible assets to value and recover. Recent Indian analysis literature identifies practical threats, including the Jet Airways CIRP in which the data in loyalty programs was disclosed through virtual data rooms without any anonymization or consent and could be compromised, or the IBBI 2021 leak of thousands of Aadhaar and PAN numbers. In India, the practitioners of insolvency (or Resolution Professionals, abbreviated as RPs) need unrestricted but controlled access to such information to meet the requirements of the statute, such as checks on claims under the IBC Section 18, asset maximization under the IBC Section 25, and the creation of resolution plans to the Committee of Creditors (CoC). The Digital Personal Data Protection Act, 2023 (DPDP Act), of India not only designates IPs as data fiduciaries but also places strong consent and minimisation requirements on them, which frequently conflict with the disclosure imperatives of IBC, but the retained GDPR (post-Brexit) of the UK gives IPs several viable processing grounds and industry-specific advice by the Information Commissioner's Office (ICO). The underlying issue of the research is that the consent-centric nature of DPDP does not support sufficiently the nature of the mandatory transparency requirements of IBC, which does not permit the insolvency-specific exemptions and proportionality tests of GDPR, subjecting Indian IPs to regulatory fines, compliance paralysis, and delays in their operations, in the absence of clear industry norms.

Need and Objective of Study

This research aims to achieve three main goals, namely, to outline the privacy rights and obligations of IPs in the IBC-DPDP interaction with the UK Insolvency Act-GDPR regime; to compare the legitimate grounds of data processing and the conflicts of data subjects; and to draw the actionable conclusions concerning the application of GDPR model to the harmonization of the Indian model. Research questions that will guide the study are: What are the privacy rights and responsibilities that accrue to Indian IPs under DPDP? What aspect does GDPR do better to use balanced mechanisms to regulate UK IPs? And what are the specific reforms that India can follow in GDPR to reduce DPDP-IBC tensions? The scope is narrowed down to corporate insolvency proceedings under CIRP and liquidation, using a doctrinal comparative approach without survey research or bankruptcy case analysis; shortcomings include the immaturity of the DPDP regulations enforcement and lack of any post-2025 case law. The paper is structured around a literature review, conceptual framework, analysis of the legal systems of India and the UK on a point-by-point basis, discussion of the rights of IP data and particularities of DPDP, and summarizes its findings, recommendations to the governmental regulation and future research directions.

Literature Review

The changing responsibilities of the insolvency practitioner have been well-recorded across the existing literature, with the ICSI Study Material (2025)[3] outlining the full range of duties of the RP under IBC: supporting confidentiality under Section 214 and the obligatory disclosures under Section 1003 considered by the public claims list, and UK studies by Pinsent Masons (2025)[4] explicating the responsibilities of the IP under the Insolvency Rules, especially when managing Data Subject Access Requests (DSARs) [file attachment]. The literature on data privacy in professional services highlights inherent threats as Wessels and Kokorin (2019)[5] discuss the tensions of European Insolvency Regulation (EIR 2015)- GDPR in cross-border settings, highlighting the encounters between the monetization of data assets and privacy concerns, using patient-records cases during German bankruptcy as an exemplar. Recent Indian

[3] Inst. of Co. Sec'ys of India, *Insolvency and Bankruptcy – Law & Practice*, Prof'l Programme, Group 2, Elective Paper 7.5 (2025).
[4] Pinsent Masons, Data Protection Concerns for Insolvency Practitioners, *Out-Law* (May 15, 2025).
[5] Bob Wessels & Ilya Kokorin, Cross-Border Cooperation and Communication: How to Comply with Data Protection Rules in Matters of Insolvency and Restructuring, 16 *Int'l Corp. Rescue* 98 (2019).

posts such as the ibclaw.in article by Sanya Dua (2025)[6] critiques unanonymized data sharing in CIRPs such as Jet Airways in conflict with the purpose limitation of DPDP, the CBCL NLIU (2025)[7] post reveals vulnerabilities in creditor lists and the repurposing of claims data by Information Utilities, and the GCBPP (2025) paper breaks down the area of digital asset distress, recommending safe harbours in light of 60% percent+ CIRPs where unstructured The Southern Pacific Personal Loans (2014) case law on GDPR and the UK practice, such as liquidators escaping controller status of pre-appointment data and the Green v Cambridge Analytica (2019) case on administrator liability limits, give judicial guidance on the costs of DSAR as administration expenses. Taken together, these pieces of evidence demonstrate an evident gap in research in that as the discussions around IBC-DPDP frictions and UK GDPR adaptations grow, no systematic investigation has explored the comparisons of IP privacy obligations under DPDP and GDPR in comparison to lawful bases of insolvency, proportionate evaluation, and reform proposals that can be illustrated in the context of the high data breach situation in India. This vacuum strands the development of policy, especially because digital assets are taking over the current insolvency portfolios.[8]

Research Methodology

The study is based on the comparative legal research theme and focuses on the state regulation of the data protection of insolvency practitioners in India and the UK. The first ones are statutory provisions (IBC §15-25, 214; DPDP §4-12; Insolvency Act 1986; GDPR Arts. 5-35), judicial case law, and secondary literature [citations].

The functionalist comparison establishes similarities in terms of structures, normative differences and practical implications, which derived a reform recommendation on mating DPDP with IBC mandates. Disadvantages are doctrinal attention and lack of empirical data and the new enforcement of DPDP.

Conceptual Framework

In India, insolvency practitioners create the backbone of the distress resolution process; under

[6] Sanya Dua & Manya Bansal, Navigating Data Protection in Insolvency: A Legal Analysis of IBC and DPDP Act, *IBC Law* (Sept. 10, 2025).
[7] CBCL, NLIU, Data at Risk: What Happens to Your Personal Data in a Corporate Insolvency? (2025).
[8] GCBPP Team, Digital Assets in Distress: Reconciling India's IBC with the DPDP Act (Oct. 21, 2025).

the CIRP (IBC Sections 16-36)[9], they can replace corporate debtor management, manage the proceedings, compile claims, convene CoC meetings and get the resolution plans or liquidation process underway, which is more or less replicated in the UK administration in Insolvency Act 1986. Their mandate includes central access to multifaceted information: personal identifiers (PAN, Aadhaar, addresses to creditors), employee details (salaries, provident fund details), and corporate ones (customer ledgers, transaction histories) needed to conduct forensic audits, valuation, and sell assets. Basic concepts of data privacy conceptualize such access: personal data includes identifiable information being processed by fiduciaries (DPDP) or controllers/processors (GDPR), which activates the rights of data subjects/principals to access, to correct, to erase, and to complain against lawful grounds, including, though not limited to, consent, legitimate purposes, legal requirements, or even the common good. Regulatory compliance relies on core principles such as necessity (data only needed to achieve insolvency goals), proportionality (balance privacy intrusion and creditor recovery), and minimization (only necessary information is retained), to help IPs strike a balance between transparency requirements and subject protection due to cyber vulnerabilities.

Legal Framework in India

According to IBC and IBBI Regulations Resolution Professionals are nominated by the Adjudicating Authority (Section 16), and given broad powers to assume control of assets (Section 18)[10], operate (Section 25)[11], and exercise due diligence, albeit on a confidentiality basis (Section 214)[12], which requires them not to disclose information except as necessary by law--but accompanied by compulsory disclosures such as public announcements, lists of claims, and CoC information sharing, and engagement of third-party professionals (valuers, legal advisors) The IPs become fiduciaries to security measures to protect personal data (IPs), and personal data processing is subject to consent (Sections 4-5)[13] or listed legitimate uses (such as legal compliance and judicial process), and the rights of data principals to access, correction, erasure, and grievance redressal protect the rights of data subjects; while the exemption covers government-notified allowlists, cross-border data transfers are complicated by the need to maintain an allowlist in each country, making global CIRPs challenging. This

[9] Insolvency and Bankruptcy Code, 2016, No. 31 of 2016 (India).
[10] Insolvency and Bankruptcy Code, 2016, § 18 (India).
[11] Insolvency and Bankruptcy Code, 2016, § 25 (India).
[12] Insolvency Act 1986, § 214 (U.K.).
[13] Digital Personal Data Protection Act, 2023, §§ 4–5 (India).

overlap creates tension: the disclosure required by IBC does not allow erasures to be undertaken, multi-stakeholder situations complicate consent in the situations of the distressed debtors, storage of data to facilitate proceedings conflicts with minimization, and proportionality is not addressed, so accountability measures are required to prevent the sanctions imposed by the Data Protection Board of India (DPBI)[14].

Legal Framework in the UK / EU

Under the Insolvency Act 1986[15] and Insolvency Rules[16] it is the duty of UK Insolvency Practitioners to realize assets and distribute proceeds, and to do so in the administration, liquidation, and receivership, and the data responsibilities include claim verification and stakeholder communication, supported by professional advice on the handling of DSARs and breach reporting provided by ACCA, IPA, and ICAEW. The GDPR[17] framework defines IPs as controllers when in principal mode (not processors), allowing processing on legitimate grounds such as legal obligation or legitimate interests, and data subject rights are limited in insolvency by insolvency-specific insolvency-specific guidance by ICO, which elucidates exemptions; cross-border adequacy decisions or safeguards are mandatory, and robust security/retention controls are mandatory. Practically, IPs operate staff data by contract compliantly, publish lessened creditor lists, utilize cloud processors that have Data Processing Contracts, and vigorously assess deletion/access demands, discarding general exclusion but prioritizing efficiency in administration, as held in cases, such as Southern Pacific,[18] where DSAR expenses were treated as costs[19].

Comparative Analysis: India (DPDP) vs UK (GDPR)

The regulatory philosophy of DPDP has concentrated on consent with limited legitimate purposes and judicial exceptions, creating rigidity where there would otherwise be no sectoral guidance, compared with GDPR, with multifarious bases of legal necessity, legitimate purposes, which are supplemented by the provision of insolvency advisories by the ICO so as to enable a flexible application. Being data fiduciaries, Indian IPs must confront unclear due

[14] Sanya Dua & Manya Bansal, Navigating Data Protection in Insolvency: A Legal Analysis of IBC and DPDP Act, *IBC Law* (Sept. 10, 2025).
[15] Insolvency Act 1986, c. 45 (U.K.).
[16] Insolvency (England and Wales) Rules 2016, SI 2016/1024 (U.K.).
[17] General Data Protection Regulation, Regulation (EU) 2016/679.
[18] *Re Southern Pacific Personal Loans Ltd*, [2014] EWHC 2485 (Admin).
[19] Pinsent Masons, Data Protection Concerns for Insolvency Practitioners, *Out-Law* (May 15, 2025).

diligence boundaries in DPDP in contrast to the precedent-based controller tests in GDPR (e.g. principal versus agent in Southern Pacific), and hold UK IPs more accountable to their process management. Legal justifications are an even more stark contrast: GDPR legal obligation is a strong force that still maintains the IBC-equivalent level of disclosure, whereas DPDP allows IPs only partial exemptions, increasing the risk of non-compliance. The conflicts caused by data subject/principal rights include in both--erasure versus retention- but GDPR is moderated through high refusal thresholds, unlike the absolutism of DPDP[20]. The security requirements of GDPR require comprehensive DPIA and Data Protection Officer, which exceed the generalised requirements of DPDP, and both regimes examine processor contracts but under GDPR it is required to be detailed. The cross-border regulations contrast the flexibility of GDPR in adequacy/safeguard with the restrictive allow-lists of DPDP, which may put Indian global resolutions on hold. Transparency requirements show that IBC has irresponsible publications that conflict with the ethos of GDPR of minimization, which highlights the transparency over privacy bias in India. On the whole, the maturity of GDPR provides IPs with the clarity of operations, showing the insolvency naivety of DPDP.

Rights of Insolvency Practitioners Over Data (India vs UK)

Under the Insolvency and Bankruptcy Code, 2016 (IBC), insolvency practitioners also called Resolution Professionals (RP) have wide statutory rights to access, process and utilize a wide range of personal and financial information necessary to the Corporate Insolvency Resolution Process (CIRP). The IBC in section 18 expressly authorises RPs to seize all assets including books of account, records and digital databases containing employee information such as salary structure, contributions to the provident fund and employment contracts, as well as creditor information (including PAN number, Aadhaar and address information to verify claims), and customer information (such as transaction history and loyalty program records) that on many occasions will form valuable intangible assets in contemporary CIRPs. This access is not just authoritative but mandatory to complete fundamental functions under Section 25 such as collating claims based on the public announcement (Section 15), preparing information memoranda to be distributed to the Committee of Creditors (CoC) and assisting with valuation by appointed experts. It is the unquestioned right of RPs to disclose this data to third parties, including legal counsel, charted accountants and application of proposed resolution (Section

[20] Sanya Dua & Manya Bansal, **Navigating Data Protection in Insolvency: A Legal Analysis of IBC and DPDP Act**, *IBC Law* (Sept. 10, 2025).

43) or undervalued transaction (Section 45) or fraudulent transaction (Section 66) to facilitate investigations, forensic audit to uncover preferential transaction, undervalued transaction, or fraudulent trade, and money monetization through invitation of resolution plan. Most importantly, the Digital Personal Data Protection Act, 2023 (DPDP Act), permits RPs to decline data principal requests to erase data under the legitimate use exemption of the judicial or legal process as insolvency proceedings are considered quasi-judicial in front of the National Company Law Tribunal (NCLT). Disclosure to CoC, courts or Insolvency and Bankruptcy Board of India (IBBI) is also safeguarded and there is continuity in proceedings without the proceedings being halted by individual privacy claims. Moreover, the RPs have rights to data retention after resolution due dates in post-facto audits or even litigation as long as they are minimally limited by the general principles of minimization[21].

In relative terms, UK Insolvency Practitioners (IPs) in the Insolvency Act of 1986 and Insolvency (England and Wales) Rules of 2016 reflect such entitlements with an enhanced legal framework under the retained GDPR. Analogous datasets, which IPs in administration or liquidation use to adjudicate claims and realizes assets, include employee payrolls, creditor ledgers containing National Insurance numbers, and customer databases, pursuant to Article 6(1)(c) legal obligation or Article 6(1)(f) legitimate interests, are lawful bases. The courts in Southern Pacific Personal Loans Ltd (2014) confirm that IPs may engage in pre-appointment data processing in the role of an agent, and the court in Green v Group Ltd (2019) restricts post-appointment principal conduct, which permits a vigorous data sharing with creditor committees, forensic examination of wrongful trading (Insolvency Act Section 214), and expert valuation. The UK IPs clearly decline Data Subject Access Requests (DSARs) or erasure requests when manifestly unfounded or excessive according to GDPR Article 12(5), to protect disruptive claims against proceedings. Disclosure rights against non-compliance with regulatory requirements are absolute to disclose to courts, creditors, or the Insolvency Service and sharing via Data Processing Agreements (DPAs) is acceptable, though the processor must be accountable.

Restrictions are heavily different: DPDP constrains Indian RPs by consent primacy (Sections 4-5) and severe minimisation (Section 8), without any express carve-out of insolvency, and threat of DPBI sanctions against perceived overreach, since there is no Indian variant of the

[21] Insolvency & Bankruptcy Bd. of India (Insolvency Resolution Process for Corporate Persons) Regulations, 2016 (India).

GDPR sectoral advisory to the ICO. UK IPs, in their turn, sail by DPIA requirements of high-risk processing (Article 35) and accountability in detail (Article 5), yet case law offers operation security, cushioning against penalties as much as 4% of worldwide turnover. Both grant audits in forensic situations, but in India by the use of RP powers (Regulation 35 IBBI), and in the UK by Section 236 investigations but the legitimate interests balancing test (Article 6(1)(f)) in the UK provides a better measure of proportionality. Resemances in employee data rights are that Indian RPs disclose PF information to CoC without granular consent, which may amount to the violation of the purpose limitation under DPDP, and UK IPs disclose information to their employers in accordance with the exceptions of employment laws (GDPR Recital 155). Finally, both regimes are more focused on insolvency efficacy, but the UK has a broader, more judicially-tested set of rights given to IPs, with inbuilt protective measures, which puts Indian practitioners in an ambiguous position facing a higher litigation risk in the early days of DPDP enforcement[22].

Challenges Faced by Insolvency Practitioners Under DPDP Act

Under the Digital Personal Data Protection Act, 2023 (DPDP Act), Indian insolvency practitioners face systemic problems with complex and intertwined consequences due to its consent-based design, not well suited to the time-sensitive, stakeholder-compounding demands of the Insolvency and Bankruptcy Code, 2016 (IBC) regime. First and most obvious is the impossibility of express consent in the case of CIRP (DPDP Sections 4-5), where corporate debtors are frequently incapacitated, directors ousted (IBC Section 17), and creditors in the thousands of cases (granular approvals, because of the logistical impossibility of such approvals within 180-day time frames, Section 12). Immediate processing of creditor claims lists, employee databases, and customer records is required in order to make public invitations (Section 15) and CoC formation, but the collective recovery paradigm of insolvency is excluded by the deemed consent of DPDP. Such a blank puts RPs in a compliance dilemma as they may face a risk of proceedings being invalidated or sanctions imposed on DPBI up to 4 percent of their turnover (Section 28).

The ambiguous exemptions of IBC functions are also annoying: where DPDP Schedule exempts judicial proceedings, CIRP quasi-judiciality in front of NCLT is not explicitly acknowledged in the GDPR, unlike the specific exemptions of insolvency carve-outs. The

[22] Pinsent Masons, Data Protection Concerns for Insolvency Practitioners, *Out-Law* (May 15, 2025).

required disclosures, including public announcements about the specifics of the debtor, claims portal revealing PAN/Aadhaar, contradict confidentiality obligations (IBC Section 214), and the purpose limitation (DPDP Section 6) since information is moved to verification to monetization through virtual data room, which occurs in Jet Airways[23] when unanonymized loyalty devices are launched, triggering concerns about breaches. Disclosure requirements increase conflicts: Section 15 publications, which are available throughout the country, discredit data minimization (DPDP Section 8) and erasure rights (Section 12) in which principals demand deletion during the middle of the CIRP and freeze asset sales and investigations of biased deals (IBC Section 43).

Another point of impasse is the data retention, where IBC requires documentation to be retained to support appeals, audit, and liquidation (up to 330 days), but DPBI (Section 9) prohibits data retention after the purpose, which pits RPs in a position of dual liability; IBBI penalties on non-retention (Section 217) and DPBI fines. It is only made more hazardous by sharing by third parties: RPs are signing valuers, lawyers, and resolution applicants (Regulation 35 IBBI), though without mandatory Data Processing Agreements like GDPR Article 28 accountability would be gone, especially when it comes to cross-border transfers limited to government allowlists (DPDP Section 16) to freeze global CIRPs (IBC Sections 234-235)[24].

Small and mid-tier IPs, which constitute 70 percent of the 5,000 plus registrants in IBBI are disproportionately burdened: they have no resources to fund security audits (Section 10), grievance mechanisms or DPIAs, unlike corporate giants. The lack of sector-specific IBBI-DPBI guidelines (as opposed to ICO playbook on insolvency) puts practitioners in interpretative gaps, which discourages involvement and adds 20-30 percent to CIRP expenditure according to NASSCOM estimates. Public leaks, such as the 2021 Aadhaar leak of IBBI, emphasize the dangers of enforcement, creating a culture of compliance paralysis, in which RPs withhold information, procrastinating decision-making and undermining the credibility of the authorities. Courts underdevelopment makes matters worse: there is no case law in the NCLAT explaining fiduciary status of RP, although the Southern Pacific case law is very clear in the UK. All these frictions jeopardize the efficacy of IBC, and thus urgent

[23] Sanya Dua & Manya Bansal, Navigating Data Protection in Insolvency: A Legal Analysis of IBC and DPDP Act, *IBC Law* (Sept. 10, 2025).
[24] Insolvency and Bankruptcy Code, 2016, §§ 15, 17, 18, 25, 214, 234–235 (India).

regulatory construction will be required to prevent practitioner turnover and chronic suffering[25].

Conclusion

This discussion reveals the rigid and consent-based nature of DPDP in its inappropriateness to the demands of insolvency, in comparison with the pragmatic multi-basis model of GDPR, ICO principles, and judicial transparency, which enable UK IPs without undermining recovery. Some of the key distinctions include narrow exemptions and general lawful causes, generic protection and DPIAs, and no sectoral guidelines and customized guidelines, which highlight India in its regulatory stage of adolescence and jeopardizes efficiency degradation as digital assets keep multiplying. Sector-specific regulation is something that arises in an imperative manner to protect the value maximization at IBC and the privacy dignity. The government role is crucial: issue joint IBBI-DPBI guidelines that reflect the exemptions on insolvency, anonymised disclosures, DPIAs on high-risk CIRPs, and obligatory RP training; revise DPDP Schedules to legalise judicial/IBC procedures, and create a special insolvency privacy sandbox, such as secure virtual data rooms. These highly moderated reforms, which are derived on the UNCITRAL ethos, will create a more harmonized framework that will enhance confidence of practitioners and a global orientation. The future research state implies empirical investigations of the compliance cost of CIRP, the post-reform breach rates, and the longitudinal outcome of the resolution.

[25] GCBPP Team, Digital Assets in Distress: Reconciling India's IBC with the DPDP Act (Oct. 21, 2025).