



DPDP Act & Arbitration: Navigating India's Evolving Data Dispute Landscape



Introduction

The digital age, while showering us with unprecedented conveniences, has also unveiled a Pandora's Box of challenges, chief among them being the pervasive issue of data privacy. As our lives increasingly migrate online, so too does our personal data, creating fertile ground for potential misuse and, consequently, a surge in data privacy disputes. In India, the judiciary has consistently championed the sanctity of personal data, recognizing its protection as a cornerstone of individual privacy. This commitment reached a zenith with the landmark 2019 Supreme Court ruling in **Justice K.S. Puttaswamy (Retd) vs Union of India**¹, which unequivocally declared the right to privacy a fundamental right. The Court, in its foresight, also underscored the pressing need for a comprehensive data privacy law, a vision that ultimately materialized with the enactment of the **DPDP Act**².

Coincidentally, India's arbitration landscape has witnessed a remarkable evolution, positioning itself as a preferred mechanism for dispute resolution. A PwC report reveals a striking preference for arbitration over traditional litigation among Indian companies, with a staggering 91% favoring it. This growing inclination towards arbitration, marked by its efficiency and confidentiality, naturally leads us to a fascinating intersection: how do



these two evolving legal frameworks – data privacy and arbitration – interact, particularly when it comes to resolving disputes arising from the digital realm?

The Arbitrability Conundrum: Can Data Privacy Disputes Find a Home in Arbitration?

The immediate question that springs to mind is whether disputes concerning data privacy, inherently sensitive and often involving public interest, can be effectively resolved through the private channels of arbitration. The DPDP Act, while establishing the **DPB**³ as a quasi-judicial body for contraventions, surprisingly doesn't explicitly bar arbitration. In fact, **Section 31 of the DPDP Act** even encourages alternative dispute resolution (ADR) mechanisms, including mediation. This subtle omission raises a crucial point: if civil courts are explicitly excluded, and arbitral tribunals are not considered "courts" in the traditional sense, then a fertile ground for arbitration in data privacy matters seemingly exists.

But the path to arbitrability isn't without its nuanced turns. Indian courts, particularly in the seminal **Vidya Drolia v. Durga Trading Corporation**⁴ case, have meticulously crafted a four-fold test to determine whether a dispute is arbitrable. Disputes are deemed non-arbitrable if they involve rights affecting the public or third parties (rights in rem), require a centralized decision, relate to the state's sovereign functions, or are explicitly or implicitly prohibited by law.

This is where the plot thickens for data privacy disputes. Are they purely contractual, involving rights in personam (enforceable between specific parties), and thus perfectly suited for arbitration? Or do they touch upon broader societal concerns, hinting at rights in rem, thereby making them non-arbitrable? Consider a scenario where a data breach impacts millions of individuals. While contractual breaches between a data fiduciary and a data processor might be arbitrable, the broader public interest in data protection and the potential for widespread harm could push such a dispute into the non-arbitrable domain. This delicate balance between private contractual obligations and public policy implications will undoubtedly be a key area of future judicial interpretation.

Beyond the Legal Labyrinth: Why Arbitration Might Be the Digital Disputes' Dark Horse

Assuming a data privacy dispute clears the arbitrability hurdle, what makes arbitration a compelling choice for parties entangled in such matters? Three critical factors emerge: compensation, confidentiality, and party autonomy.

Compensation: A Missing Piece in the DPDP Puzzle?

Perhaps the most significant allure of arbitration in data privacy disputes stems from a perceived lacuna in the DPDP Act itself: the absence of clear provisions for awarding





compensation to aggrieved parties. While earlier drafts hinted at such remedies, the final DPDP Act primarily focuses on imposing penalties for contraventions. This leaves victims of data breaches in a peculiar predicament: they can lodge a complaint with the DPB, which may impose fines, but direct financial recompense remains elusive.

Here, contractually induced arbitration agreements become invaluable. Imagine a data processing agreement between two companies. If one breaches its security obligations leading to a data leak, the aggrieved party, through arbitration, can seek compensation for damages incurred, a remedy not explicitly guaranteed by the DPDP Act's current framework. While **Section 27(1)(a) of the DPDP Act** mentions the DPB's power to direct "urgent remedial measures," whether this encompasses compensation remains an open question, awaiting clarification through rules or judicial pronouncements. Until then, arbitration stands as a more direct route for financial redress.

Confidentiality: A Sanctuary for Sensitive Data

In the realm of data privacy, where sensitive personal information is constantly in play, confidentiality isn't just a preference; it's a necessity. Traditional court proceedings, by their very nature, are public, potentially exposing intricate details of data breaches and related sensitive information to a wider audience. This can lead to reputational damage, competitive disadvantages, and further privacy concerns for the parties involved.

Arbitration, in stark contrast, offers a haven of privacy. **Section 42A of the Arbitration Act⁵**, imposes a binding obligation on all participants – arbitrators, institutions, and parties – to maintain the confidentiality of proceedings and documents. This inherent secrecy aligns perfectly with the core objective of the DPDP Act: the protection of personal data. When sensitive databases, proprietary algorithms, or personal identifying information are central to a dispute, the closed-door nature of arbitration provides an invaluable shield. Even though arbitral tribunals enjoy certain exemptions from DPDP Act compliance requirements under Section 17(1)(b), they remain firmly bound by the obligation to provide reasonable safeguards against data breaches under Section 8(5), ensuring that the sanctity of personal data is upheld even within the private arbitration ecosystem.

Party Autonomy: Tailoring Justice to Data's Nuances

One of the cornerstones of arbitration is party autonomy, empowering disputants to shape the process to their specific needs. This flexibility extends to choosing the arbitral institution, the procedural rules, and, crucially, the arbitrators themselves. In the highly specialized domain of data privacy, this autonomy is a game-changer. Parties can handpick arbitrators with deep expertise in data protection laws, cybersecurity, and information technology – a



level of specialized knowledge that might not always be readily available in general civil courts. This ensures that disputes are adjudicated by individuals who truly understand the complex technical and legal nuances of data privacy, leading to more informed and efficient resolutions.

The Road Ahead: A Cautiously Optimistic Outlook

The interplay between India's burgeoning data privacy framework and its evolving arbitration landscape presents a compelling narrative. While the DPDP Act lays down the foundational principles for data protection, arbitration offers a potentially more agile, confidential, and compensatory pathway for resolving disputes. The journey, however, is not without its challenges. The ongoing evolution of arbitrability jurisprudence, particularly concerning the in rem versus in personam nature of data privacy rights, will be critical.

How will the Indian legal system reconcile parallel proceedings – a complaint before the DPB focused on penalties, and an arbitration seeking compensation? Will the courts develop clear guidelines to delineate the jurisdiction of each? And how will the increasing integration of Artificial Intelligence (AI) in arbitration, as highlighted in the provided abstract, further shape the resolution of data disputes? AI tools, with their capabilities in document review, predictive analytics, and even virtual arbitration, promise to streamline processes and enhance efficiency. However, they also introduce new layers of complexity concerning data privacy within the arbitral process itself, demanding robust safeguards and ethical considerations.

The future of data privacy dispute resolution in India appears to be a dynamic and fascinating space. By thoughtfully integrating the strengths of arbitration – its speed, confidentiality, and flexibility – with the robust principles of the DPDP Act, India has the potential to forge a dispute resolution ecosystem that not only safeguards personal data but also offers efficient and effective remedies to those whose digital rights are breached. The stage is set for a captivating evolution, and observing how this intricate dance unfolds will be truly insightful.

Citations

1. Justice K.S. Puttaswamy (Retd) vs Union of India 2019 (1) SCC 1
2. Digital Personal Data Protection Act, 2023
3. Data Protection Board of India
4. Vidya Drolia v. Durga Trading Corporation 2021 2 (SCC) 1
5. Arbitration and Conciliation Act, 1996

Expositor(s): *Adv. Anuja Pandit*
