

Consent Continuity: Where corporate and data privacy laws clash

The enactment of India's Digital Personal Data Protection Act, 2023 (DPDP Act) has tightened the screws around consent requirements by mandating that consent from data principals be free, specific, informed, unconditional and unambiguous. While these are critical in rightfully empowering data principals, the DPDP Act does not completely deal with how consent is to be treated when a business that is in possession of personal data is acquired.

The Hon'ble Supreme Court of India, in Justice K.S. Puttuswamy v. Union of India, held that privacy is a fundamental right protected under Articles 14, 19 and 21 of the Constitution. The judgment affirmed the need for individuals to have control over dissemination and use of information relating to them. Under corporate and contract law principles, assets, liabilities, contracts, employees and operational rights are considered transferable to successor or surviving entities. Personal data records are paramount to commercial continuity of business and are typically assumed to be a business asset.

This brings us to the key question: Does consent obtained by an entity automatically survive when the business is taken over, acquired or merged with another entity?

Corporate Succession vs. Data Principal Consent

From a corporate law perspective, the successor entity steps into the shoes of the transferring entity. Hence, what is critical is whether consent is a transferable incident of the database being transferred?

Based on the Puttuswamy judgment, it can be argued that personal data is not merely an asset. The individual's privacy interest continues even when the database changes hands. Under the DPDP Act, consent is a specific contract between the data fiduciary and the data principal. Consent is closely linked to the identity of the data principal, and the purposes for which personal data is processed. The DPDP Act does not expressly resolve how these principles interact during business transfers. This raises a dual concern – whether the surviving entity has a legal right to take possession and control of the personal data and whether the surviving entity has a lawful basis to process such personal data after the transaction.

Carve-outs under the DPDP Act

The DPDP Act provides carve-outs for when certain provisions of the DPDP Act, particularly those relating to consent, shall not apply. One of those carve-outs is a court or tribunal approved scheme of compromise or arrangement or merger or amalgamation of two or more companies or a reconstruction by way of demerger. Accordingly, the DPDP Act does acknowledge a situation where corporate restructuring may require transfer of personal data; however, it limits the carve-out to court approved schemes. There is no carve-out for slump sales, asset transfers, etc. where a transfer of business is taking place outside of the court. In today's times, such transactions are par-for-course, more so in businesses that are heavy on possessing personal data, that are typically asset light businesses.

With the DPDP Act limiting the carve-out to court approved schemes, there is a lacuna for the legal treatment of consent obtained with respect to data transferred as part of privately negotiated business transfers. In the absence of this, it leads to the practical impossibility of going back to the customers/consumers (especially in B2C models) and seeking consent for the business transfer.

Another grey area in the consent-sphere is IBC driven acquisitions, either through a liquidation sale or an asset sale. In a liquidation sale, the liquidator is required to realize the company's assets to maximum value. Accordingly, can the customer database of a company be sold as an asset? While the carve-out in the DPDP Act covers actions approved by 'any competent authority', it does not specifically contain a liquidation or asset sale as a specific transaction for which the carve-out shall apply.

Considering the lack of clarity on privately negotiated transfer and IBC liquidation sales, companies often rely on consent language in their privacy policies to hedge the risk. This brings us to the concept of 'consent framework'.

Consent Framework

Historically, the most common practice to address this has been to include language in privacy policies, whereby consent of the data principal is obtained upfront to transfer their data as part of corporate restructuring, including mergers, acquisitions and slump sales. A common formulation defines the term "company," "we," or "our" broadly to include the parent company, subsidiaries, affiliates, or entities within the same corporate group.

Under the DPDP Act, the agreement between data fiduciary and data principal is for processing of personal data for a specified purpose and is limited to such personal data as is necessary for such specified purpose. The DPDP Act further mentions that any consent that does not comply with such requirements will be considered void (even if the user has consented to such provision).

The argument that the consent continues if the privacy policy has a broad language is defensible when the transfer is between group companies. If both the parent and subsidiary were already disclosed collectively as part of the relevant processing ecosystem, the parent is less likely to be characterized as an undisclosed third party suddenly assuming control over personal data.

However, when data is transferred to an unrelated entity, can consent be extended to be valid where the data principal is not aware of the identity of the transferee?

This brings us to the concept of due diligence and continuity of purpose.

Due diligence and Continuity of Purpose

In the absence of detailed jurisprudence or regulatory guidance under the DPDP Act, the principles of prudence and defensibility become important. Accordingly, privacy due diligence becomes important in such transactions. It is important to analyse whether the terms are broad enough to cover such consent and whether such consent is likely to be valid. Depending on the findings of privacy due diligence and nature of personal data concerned, a call needs to be taken on whether prior consent of the data principals will need to be obtained.

Where consent is not being sought for transfer of ownership of data, assessing whether processing purposes will remain the same post-closing becomes important to mitigate the risk. If any changes are proposed to the use-case of personal data like expansion of the purpose of processing, alteration of retention practices, etc., it may be difficult to argue that the previous consent is valid. On the other hand, if the data is proposed to be used for providing the same products and services and there is no expansion to other uses, then the argument of continuity in use becomes stronger.

Mitigation by notification

Given the absence of detailed jurisprudence or regulatory guidance under the DPDP Act, transactional practices in India are evolving. From a prudence perspective, companies issue post-transaction privacy notices. In such cases, companies clarify the identity of the surviving entity, revisions to any use case, and any other privacy policy changes, post-closing of a transaction. While this should satisfy the transparency test, whether such consent is valid for the DPDP Act is yet to be tested.

A continuing grey area

The DPDP Act has fundamentally changed how businesses must think about personal data during mergers and acquisitions. While corporate law may permit transfer of databases and customer relationships through legal succession, data protection law imposes an additional layer of scrutiny focused on consent, transparency, and reasonable expectations. The result is a growing legal grey area: ownership of data may transfer through a transaction, but the lawful basis to continue processing that data may not transfer automatically or as seamlessly. Until Indian regulators or courts provide clearer guidance, organizations will likely continue relying on expansive privacy notice drafting, continuity-of-purpose arguments, and post-transaction transparency measures to navigate this uncertainty.

Authors

Saumya Ramakrishnan

Contact: saumya@bombaylawchambers.com

Disclaimer: The article is intended solely for general informational purposes only and does not constitute legal advice. It should not be acted upon without seeking specific professional counsel. No attorney-client relationship is created by reading this article.