Data Privacy in M&A: Navigating Compliance under India's DPDP Act

Mergers and acquisitions (M&A) have always been intricate processes, often requiring careful navigation of various legal, financial, and operational complexities. In today's digital landscape, however, one of the most significant challenges for businesses involved in M&A transactions is ensuring compliance with evolving data privacy laws. In India, the Digital Personal Data Protection Act (DPDP Act)—though not yet fully in force—has already begun to shape how companies handle and protect personal data, especially in the context of M&A.

While the DPDP Act is still in its implementation phase, companies involved in M&A deals must begin preparing for the eventual regulatory scrutiny it will bring. The Act mandates that any acquiring company that takes control of personal data will become the 'Data Fiduciary'— inheriting all responsibilities for the data's security, privacy, and compliance. In anticipation of the Act's full enforcement, businesses must take proactive steps to ensure they meet its stringent requirements.

A Cautionary Tale: An E-Commerce Platform's Early Data Privacy Dilemma

Consider the case of a leading e-commerce platform in India that recently completed a major acquisition. As part of the transaction, the acquiring company gained access to an extensive database of customer information, which included everything from contact details to shopping habits. The goal was to integrate the target company's data into the acquiring company's systems, creating a more unified and efficient customer experience. However, during the integration process, the e-commerce platform encountered a major challenge: data mapping had been rushed, and key data privacy protocols were overlooked.

In particular, access controls were not as robust as they should have been, leaving sensitive customer information vulnerable to unauthorized access. While this data breach occurred before the DPDP Act was in full force, it still attracted attention under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which impose stringent requirements on data protection. This breach not only caused operational setbacks but also resulted in damage to the company's reputation and consumer trust—a significant concern for any business in an increasingly data-conscious world.

While this case didn't fall directly under the DPDP Act due to its phase of enforcement, it provided an early lesson in the importance of compliance with data privacy regulations—especially as the DPDP Act looms on the horizon.

The Growing Impact of the DPDP Act on M&A

As the DPDP Act moves closer to full implementation, businesses must start thinking

about data privacy as an integral part of their M&A strategies. The Act will impose significant obligations on entities involved in handling personal data, particularly when personal data is transferred during a merger or acquisition.

Under the DPDP Act, the acquiring company becomes the Data Fiduciary. This role comes with a host of responsibilities, including ensuring that the data is processed in compliance with the principles of data minimization, purpose limitation, and data retention. The Act also stipulates that any transfer of personal data to a third party must be done under strict conditions, ensuring that the data remains secure throughout the transaction.

Furthermore, the DPDP Act mandates the informed consent of data subjects. If the target company hasn't obtained clear consent from individuals whose data is being transferred or processed, the acquiring company will be responsible for rectifying this gap. This can add a layer of complexity to M&A deals, especially when dealing with large volumes of personal data.

Another critical aspect of the DPDP Act is the requirement for Data Protection Impact Assessments (DPIAs). These assessments are designed to identify and mitigate risks associated with data processing activities during an M&A transaction. DPIAs are vital in ensuring that the integration process doesn't inadvertently breach data protection rules and that risks to data subjects are adequately addressed.

What M&A Participants Should Do Now

Given that the DPDP Act is on the verge of full implementation, businesses involved in M&A transactions must start preparing for its eventual requirements. The following steps can help ensure compliance and reduce risk during the integration process:

1. Conduct Thorough Due Diligence: M&A transactions should include a comprehensive audit of the target company's data protection practices. Understanding the data flows, data usage, and storage practices of the target company is critical to identifying any compliance gaps.
2. Ensure Proper Data Mapping: Before integrating data systems, businesses should conduct thorough data mapping exercises to understand where and how sensitive personal data is stored, processed, and transferred. This process will help identify potential risks and ensure that personal data is handled appropriately.
3. Implement Strong Data Protection Protocols: Companies should ensure that strong access controls, encryption, and security protocols are in place to safeguard personal data during the transition. This also includes ensuring that data sharing between entities is done securely and only with the necessary parties.
4. Prepare for DPIAs: Organizations should begin conducting Data Protection Impact Assessments to evaluate the risks associated with data integration and to develop mitigation strategies. DPIAs should be conducted before any major data transfers occur during the M&A process.
5. Train Key Personnel: Senior management and key personnel involved in M&A transactions should receive training on the obligations of the DPDP Act, particularly on their role as Data Fiduciaries. This will ensure that all parties understand their responsibilities and how to implement data protection practices during the integration process.

Conclusion: Future-Proofing M&A with Data Privacy in Mind

As India moves towards fully enforcing the DPDP Act, M&A participants must recognize that data privacy will no longer be an afterthought. Instead, it must be embedded into the transaction from the very start. The evolving legal landscape makes it essential for businesses to anticipate future compliance requirements and to take proactive steps now to mitigate risks.

While the full enforcement of the DPDP Act is still on the horizon, the case of the e-commerce platform highlights the pressing need for businesses to treat data privacy with the seriousness it deserves, especially during M&A transactions. As organizations prepare for this shift, the companies that succeed will be those that recognize data privacy as an integral part of their growth strategy—not just a compliance requirement.

Authored by

Shrikrishna Dikshit
Baker Tilly ASA India

Rachit Shukla
Baker Tilly ASA India