DATA SECURITY AND PRIVACY COMPLIANCE: A CHALLENGE IN MERGERS AND ACQUISITIONS

Sejal Jain, Advocate, Rajasthan Bar Council

ABSTRACT

M&A has unique challenges in terms of data security and privacy compliance in an age where data has become one of the most significant corporate assets. M&A transactions are especially susceptible to privacy violations and cyber threats because of the extensive interchange of sensitive and personal data during due diligence, negotiations, and post-closing integration. Organisations involved in M&A are under greater scrutiny to protect personal data and set up strong compliance frameworks in light of the Digital Personal Data Protection Act, 2023 (DPDP Act) and international regulations like the GDPR. With an emphasis on the duties of Data Fiduciaries and Processors, the legal requirements under the DPDP Act, and the potential repercussions of ignoring concerns about privacy, this article examines the crucial role that data privacy plays in M&A transactions. Examining real-world scenarios like Facebook's attempt to acquire TikTok and Verizon-Yahoo Acquisition, this article highlights the adverse impact of data protection on financial, legal, and reputational issues. In order to present data privacy as a key component of successful M&A results, it concludes by offering strategic ideas for risk mitigation, such as data minimization, anonymization, contractual safeguards, and technology-enabled compliance measures.

INTRODUCTION: WHY IS DATA PRIVACY CRUCIAL IN MERGER AND ACQUISITION AGREEMENTS?

In today's business-savvy world, mergers and acquisitions are crucial instruments for industry integration and overall industry evolution. The process through which two entities combine their strengths to produce a wave of favorable results is called a merger. Given this, it is necessary to transmit the vast amount of data that has been created and stored over the years in a safe and secure manner in order to maintain the business entities' vulnerability. Herein lies the corporate world's manifestation of the data protection regime and its greatest usefulness. Apart from data protection regulations, there is no other legally binding regulation that can guarantee this kind of security and address security breaches. Corporate entities bear the fundamental responsibility of guaranteeing the implementation of whatever safety mechanisms they employ during data transfers. Nevertheless, their deficiency of statutory authority and enforcement ability renders this approach highly uncertain and flexible. This explains the essence of the issue, highlighting the urgency of data privacy laws to guarantee that multinational corporations (MNCs) maintain their worth in their markets, ward off potential risks, and take all reasonable precautions to avoid them.[1]In the present M&A landscape, a number of parties share a lot of data in order to comprehensively assess transaction risks, including the target firm, sellers, and possible purchasers. But in the midst of this cooperative process, personal data protection is frequently disregarded, especially because the Sensitive Personal Data or Information (SPDI) Rules are not strictly enforced. However, considering the upcoming Digital Personal Data Protection Act, 2023 ("DPDP Act" or "the Act") and its severe penalty framework, this negligence is unsustainable.

AN OVERVIEW OF THE ACT[2]

Following the Supreme Court's Puttaswamy ruling[3], which emphasized the need for such legislation and recognized the right to privacy as a basic right under Article 21, the DPDP Act

[1] Adarsh Gautam & Manvee, Emerging Data Privacy Concerns in Mergers & Acquisitions Deals: Tackling Regulatory Apprehensions, *TAXMANN* (July 23, 2023), https://www.taxmann.com/research/company-and-sebi/top-story/105010000000023139/emerging-data-privacy-concerns-in-mergers-acquisitions-deals-tackling-regulatory-apprehensions-experts-opinion.

[2] Chinmay Verma, Data Protection in M&A Transactions, *PRIVACY DESK* (Mar. 14, 2022), https://privacydesk.in/publications/articles/data-protection-in-ma-transactions/#:~:text=Data%20Protection%20and%20Privacy%20Legislations%20for%20M&A%20in%20India&text=Information%20Technology%20(Reasonable%20Security%20Practices,corporates%20as%20well%20as%20individuals.

[3] K.S. Puttaswamy and Anr. vs. Union of India, ((2017) 10 SCC 1).

functions as a complete piece of legislation for protecting personal data. The General Data Protection Regulation ("GDPR") of the European Union serves as the model for several aspects of the Act, some of which have been modified for the Indian environment. In other words, the DPDP Act defines Personal Data as any digital information concerning an identifiable individual and defines it as such for all purposes, regardless of sensitivity.[4]

In addition, the Act lists the three main players in the data ecosystem. The person to whom the data relates is the Data Principal, who comes first.[5] The second party is the Data Fiduciary, who is accountable for deciding how and why to process the data and is susceptible to fines and other compliance-related procedures.[6] Last but not least is the Data Processor, who serves as the Fiduciary's agent or service provider and is not directly liable.[7] According to Section 4 of the Act, "processing" of Personal Data must be limited to the consent-notice framework or other permissible uses.[8] As a result, data processing can only take place with the Data Principal's permission, for the reasons allowed by Section 5[9], and with or before a notice. However for the legitimate uses listed in Section 7, there may be an exemption to this consent-notice framework.[10]

PERSONAL DATA CONCERNS DURING AN ACQUISITION

During an M&A deal, parties exchange copious amounts of data on the target firm with their advisors, including legal counsel and financial auditors. The due diligence process is sparked by this information exchange, which is typically made possible by virtual data rooms. Personal data, including employment contracts, contracts with suppliers or vendors, and personal data of staff members, clients, directors, etc., are also shared. Under the terms of the Act, any information of this kind exchanged between the parties to the transaction is considered "processing."[11]

What Part Do All Parties Play?

The question that arises in light of the processing of Personal Data that occurs during the

[4] Digital Personal Data Protection Act, 2023, § 2(t), No. 22, Acts of Parliament, 2023 (India).
[5] Digital Personal Data Protection Act, 2023, § 2(j), No. 22, Acts of Parliament, 2023 (India).
[6] Digital Personal Data Protection Act, 2023, § 2(i), No. 22, Acts of Parliament, 2023 (India).
[7] Digital Personal Data Protection Act, 2023, § 2(k), No. 22, Acts of Parliament, 2023 (India).
[8] Digital Personal Data Protection Act, 2023, § 4, No. 22, Acts of Parliament, 2023 (India).
[9] Digital Personal Data Protection Act, 2023, § 5, No. 22, Acts of Parliament, 2023 (India).
[10] Digital Personal Data Protection Act, 2023, § 7, No. 22, Acts of Parliament, 2023 (India).
[11] Digital Personal Data Protection Act, 2023, § 6, No. 22, Acts of Parliament, 2023 (India).

transaction relates to the role that each data processing party assumes in these situations—that is, whether they perform the functions of a Data Processor or a Data Fiduciary. Making this distinction is important since both the Data Processors' and Data Fiduciaries' acts carry obligations.

The target or seller clearly acts as a Data Fiduciary when it provides Personal Data to the bidder or acquirer. Crucially, this step also obliges the purchaser to assume the equivalent of a data fiduciary duty. This is so that it can determine if the transaction is feasible by processing the Personal Data in accordance with its intended use and means. As a result, in this scenario, both the target and the acquirer will be accountable for adhering to the Act in their respective capacities. However, this categorization is flexible and dependent on the conduct of the individuals concerned. As a result, it is advised that the parties clearly state in their pre-merger documents what their respective roles are as well as the need for data sharing. Additionally, under the Act, advisors to either party who review the documentation and Personal Data in order to provide professional opinions would be considered Data Processors.[12]

The Foundation of Data Processing

Processing Personal Data for the "legitimate interests of the data controller" (i.e., akin to a Data Fiduciary) is allowed under the GDPR. Therefore, parties to an M&A transaction may treat Personal Data without seeking new consent or taking into account outside factors if they are able to balance their interests against those of the Data Principal. Interestingly, the 2022 Data Protection Bill approved the processing of Personal Data as a permissible use for corporate restructuring, mergers, and acquisitions, thereby making the consent-notice structure obsolete.[13]

The current version of the Act, however, only exempts the application of some of its provisions, such as the grounds for processing under Section 4, when the processing is done in accordance with corporate actions approved by a court or tribunal, like compromise, arrangement, merger, amalgamation, reconstruction, or transfer of undertaking between companies.[14] As a result, the

[12] Rahil Arora & Vidushi Sehgal, Navigating M&A Transactions Amidst the Digital Personal Data Protection Act, *Centre for Business and Commercial Laws, NLIU Bhopal* (Jan. 27, 2024), https://cbcl.nliu.ac.in/mergers-acquisitions/navigating-ma-transactions-amidst-the-digital-personal-data-protection-act/#:~:text=Interestingly,%20the%202022%20Data%20Protection,to%20the%20consent-notice%20framework

[13] *Id.*

[14] Digital Personal Data Protection Act, 2023, § 17(1) (e), No. 22, Acts of Parliament, 2023 (India).

Act's requirements for consent and notice before sharing Personal Data with a third party would apply to any other non-court-approved transaction, like the transfer of shares or other assets.

Actions to Consider

A very severe penalty system for violations of personal data is introduced by the DPDP Act, with penalties for Data Fiduciaries reaching INR 250 Crs.[15] In light of this, Data Fiduciaries are required to carefully carry out their Act-related duties. The first step entails determining whether the processing of Personal Data is in line with the purpose for which the Data Principal's consent was previously acquired. If the processing goes beyond the intended use, it will be essential to get new consent from the data principals and comply with notification obligations before processing the data. If the business finds it difficult to get new or prior consent, it must anonymize or pseudonymize Personal Data before disclosing it. Furthermore, it is important to think about whether processing employee data during an M&A transaction qualifies as legal use "for the purposes of employment."[16] The boundaries of this kind of legal use are still unclear, but in order to reduce the dangers, it is best to get the right kind of employee agreement before processing anything, with valid use acting as a buffer.

In addition, it is essential to follow the DPDP's guidelines for data minimization and purpose limitation when revealing Personal Data. This means that instead of providing the acquirer with an excessive amount of information, the processing of Personal Data must be limited to that which is necessary to make an investment decision regarding the target. In accordance with these guidelines, the target may decide to reveal Personal Data gradually or hold off until closing, particularly when it comes to workers. According to the Act, it is essential to guarantee the consistency, correctness, and completeness of the data that is revealed. The acquirer is likely to pursue this need by representations and warranties.

In order to reduce risk, even though both parties are acting as Data Fiduciaries, they should sign Non-Disclosure Agreements (NDAs) that abide by the DPDP Act. The grounds and conditions of data processing, purpose restriction, data retention, security measures, notification requirements, form and timeliness of disclosure, and any other organizational and technical measures to be put into place should all be outlined in NDAs. It is imperative that both parties guarantee the erasure of Personal Data by themselves and their Data Processors

[15] Digital Personal Data Protection Act, 2023, Sch., No. 22, Acts of Parliament, 2023 (India).
[16] *Id.* at 10.

upon completion of the intended purpose or consent withdrawal. With respect to the international transfer of Personal Data for processing, a blacklisting strategy that limits transmission to specific designated jurisdictions has been implemented. Therefore, before participating in any transfer of Personal Data, targets should take this into account in addition to any sector-specific constraints. Lastly, as advisers hired by the parties are considered Data Processors, the parties should try to pass along specific obligations and impose stricter compliance requirements to reduce the advisors' liability, in addition to ensuring that their employment is based on a legitimate contract.[17]

POSSIBLE PRIVACY CONCERNS RESULTING FROM MERGERS AND ACQUISITIONS

During the whole M&A transaction life cycle, acquiring companies need to be extremely aware of privacy and security issues. From the beginning, it's critical to establish precise business objectives, comprehend data usage methods, and recognize potential hazards. Erroneous assumptions about rights and constraints might lead to downstream hazards if data aims are not understood beforehand.[18]

1. The Phase of Due Diligence

In this stage, an extensive privacy and security risk assessment that goes beyond a typical framework must be carried out by the acquiring entity. This means figuring out the commercial justifications for the purchase as well as any compliance concerns, especially with relation to the consumer consent that was acquired for data sharing. In addition, assessing culpability for privacy or data breaches is essential to figuring out post-acquisition obligations. It is also necessary to take into account how the new entity will fit into the larger organizational framework, including details like data localization, third-party participation, and data transfer methods.

2. The Phase of Regulatory Approval

Regulatory bodies carefully examine mergers and acquisitions for their effects on competition and may call for corrective action. But these solutions might be in violation of

[17] *Id.* at 12.
[18] *Id.* at 1.

privacy rules, which would make closing the purchase difficult. It is even more crucial to carry out thorough due diligence before requesting regulatory approval in order to foresee and resolve such conflicts.

3. The Integration and Post-Closing Phase

Remedial actions for non-compliance issues found during the deal's lifespan should be prioritized, with an initial focus on high-risk areas. Businesses must to reevaluate their responsibilities, especially in situations when there are several data protection laws, like the GDPR. It could be required to implement mitigation techniques, like ring-fencing, to lessen the chance of data contamination. Additional precautions to reduce risks during the integration process include obtaining new consent and putting updated privacy warnings into place.

Mitigating Data Privacy Concerns in Mergers and Acquisitions

1. Comprehending Your Data

- Data Mapping: Make a detailed analysis of the information environment to understand the different kinds of data, where they are stored, and how they are processed. As a result, data governance is enhanced and downstream risks are lessened.

- Policy and Procedure Alignment: To guarantee coherence and correct any inconsistencies with compliance, review and update the privacy, security, information governance, and trade secret handling policies.

2. Overseeing New Data Sources

- Diverse Data Handling: Get ready to handle data that comes from multiple platforms for streaming, collaboration tools, and communication channels. This will require customized solutions for data search, gathering, and management.

3. Simplifying the Procedures for Data Review

- Merger Clearance Investigations: Be prepared for increased regulatory scrutiny, which calls for the prompt disclosure of a wide range of internal records and information.

Utilize technology-enabled review instruments such as predictive coding to accelerate the review procedure.

4. Using Technology to Ensure Constant Compliance

- Data Identification and Classification: To protect sensitive information and expedite compliance activities, employ solutions for data identification and classification.

- Data Loss Prevention: Put policies and procedures in place to guard against data leaks and guarantee the safe management of important intellectual property.

- Digital Rights Management: Make use of tools to protect and manage digital rights, which will improve data privacy and compliance.[19]

DATA BREACH AND CYBERSECURITY CONCERNS IMPACTING PROMINENT M&A TRANSACTIONS

Verizon Acquires Yahoo[20]

A data leak also led to the cancellation of Verizon's proposed acquisition of Yahoo. In the course of the two firms' negotiations, Yahoo revealed two distinct instances of data breaches. 500 million user data records were compromised in the first breach, which was the result of a hacker; the second breach touched the data of about 1 billion users. Both breaches led to the loss of users' personal information and login passwords. Verizon's actions decreased Yahoo's worth by around $350 million even if the deal went through.

Facebook's Attempted Acquisition of TikTok[21]

Musical.ly, which was eventually rebranded as TikTok, was a well-known app for quick music and entertainment videos. Facebook, one of the biggest social media networks, was in the process of acquiring the app. But it took several months for a decision to be made, and in the end, Facebook pulled out of the agreement, citing two main reasons: First, the fact that TikTok started out as a Chinese software caused some concern. Secondly, the content of the site was

[19] *Id.*
[20] Jon Porter, Yahoo is Yahoo once more after new owners complete acquisition, *THE VERGE* (Sept. 2, 2021), https://www.theverge.com/2021/9/2/22653652/yahoo-aol-acquired-apollo-global-management-private-equity.
[21] *Id.* at 1.

judged to be against American regulations that safeguard children's internet privacy. The deal was then pursued by ByteDance, another American business. As per Reuters sources, TikTok had cybersecurity issues and was scrutinized by the Committee on Foreign Investment in the United States due to possible national security implications after being acquired by ByteDance.

Driven by worries about the safety of Americans' personally identifiable information, CFIUS forced Kunlun Tech Co Ltd to sell the gay dating app Grindr last year and blocked Ant Financial of China's attempt to buy MoneyGram in 2017. These occurrences highlight how crucial it is to give data protection top priority in international M&A transactions.

CONCLUSION

Data privacy has become a major factor in determining the viability and success of deals, as the present-day M&A environment demonstrates. Following the DPDP Act and other international frameworks has become essential as transactions depend more and more on the safe interchange and legal processing of personal data. If data security is not given first priority, both buyers and sellers may be subject to harsh legal penalties, a decline in market value, and a breakdown in stakeholder confidence. On the other hand, taking proactive steps, such as defining fiduciary duties clearly, conducting thorough due diligence, using anonymization techniques, and enforcing stringent contractual obligations, can greatly lower risks and improve transactional integrity. The lessons learnt from well-known M&A failures indicate that ignoring privacy is a strategic vulnerability as well as a compliance issue. Thus, including privacy-by-design principles and incorporating data security at every stage of the deal process is not just a legal need but also an economic imperative for companies navigating mergers and acquisitions in the digital age. M&A dealmakers are now emphasizing cybersecurity more throughout the due diligence process to make sure the target company has sufficient security measures to comply with legal requirements.