

**DATA PROTECTION IN M&A TRANSACTIONS UNDER THE
DPDP ACT, 2023: A CRITICAL ANALYSIS VIS A VIS THE EU GDPR**

*Pranika Goel and Ayush Katyayana **

ABSTRACT

While the impact of the Digital Personal Data Protection Act, 2023 will be felt across multiple sectors, the authors in this article have sought to analyse how the framework envisaged by the Act plays out in the context of M&A transactions and parties thereto as data fiduciaries under the Act, particularly in light of the exemption and relaxations in favour of such transactions under Article 17(1)(e). For this, the authors also draw a comparison with the like exemption contained under Article 6(1)(f) of the European Data Protection Regulation, to conclude that relative to its EU counterpart, the exemption for M&As in India is both too narrow as well as vague and ambiguous in its amplitude insofar as it only applies to court-approved schemes of mergers and amalgamations post obtaining such approval (and not before that, or in case of private arrangements, altogether), and at the same time dispenses not only the consent requirement like the EU GDPR but a host of other obligations and safeguards under the DPDP Act, the exact ambit of which is unclear. Even the recently notified Draft Digital Personal Data Protection (DPDP) Rules, 2025 present a missed opportunity as they provide no additional guidance on the ambit and/or implementation of the M&A exemption under the Act. In light of this, the authors suggest whitelisting M&As under the legitimate uses clause enshrined in Section 7 of the DPDP Act which allows data processing without consent in the listed situations, as opposed to covering them under the Section 17 exemptions or invoking the concept of deemed consent. The authors further suggest that unlike the GDPR exemption which might be a bit too broad and subjective in its scope and application, the ambit of the M&A exemption be circumscribed by reasonable safeguards like the obligation to notify a data principal of the processing of their personal data without their consent pursuant to the exemption, and allowing data principals to object to such processing which would result in a more compelling interest for such processing having to be established vis a vis the rights and interests of the affected data principal, on the lines of what is seen under the GDPR.

Keywords: DPDP Act, DPDP Rules, Digital Data Breaches, M&A Transactions,

* Pranika Goel is an Associate at Shardul Amarchand Mangaldas & Co and Ayush Katyayana is a Final year law student at National Law University, Delhi.

Merger Exemptions.

TABLE OF CONTENTS

| | | |
|-------------|--|-----------|
| I. | OVERVIEW..... | 46 |
| II. | THE INDIAN FRAMEWORK..... | 48 |
| III. | M&A EXCEPTION UNDER THE EU GDPR..... | 50 |
| IV. | THE M&A EXEMPTION UNDER THE DPDP ACT: WHOM DOES IT REALLY BENEFIT?..... | 54 |
| V. | THE SUGGESTED ALTERNATIVE: STRIKING A BALANCE..... | 57 |
| VI. | CONCLUSION..... | 61 |

I. OVERVIEW

The importance of data protection for Mergers and Acquisitions (“**M&As**”) cannot be overstated. M&A transactions are widely resorted to by companies to acquire scale, technology, portfolio diversity, financial efficiency and the like, and the wealth of data a target company possesses is often a vital asset that sees a deal go through. Given the quantum of data collected or otherwise held and used by companies, what happens to the personal data of stakeholders like customers, employees, etc. of the merging companies (particularly the entity being acquired) assumes paramount importance during an M&A transaction.

Compliances as to data protection emerge at various stages of an M&A deal—right from ascertaining a target company’s privacy exposure at the screening stage and accounting for the potential cost of compliance/liabilities in the deal value, to the subsequent stage of data privacy due diligence preferably by way of a secured data room. This is then followed by the incorporation of data privacy aspects in the terms of the deal between the two companies, including details as to treatment and usage of data held by the two companies and consent given by principals of such data, potential liabilities arising from pre-deal data breaches by

the acquired entity, and resolution of disputes emerging therefrom. The final stage often entails the data systems of the two companies being integrated with each other post-closing of the deal in compliance with the relevant data protection regulations.

Non-compliance with data privacy measures and data breaches can often have damaging repercussions for the merging entities, including but not limited to potential liabilities and fines accruing in the future- going up to INR 250 crores in India¹, and 4% of a company's global turnover or 20 million Euros, whichever is higher, in the EU.² The most classic example of the impact of a data breach on an M&A deal would be the disclosure of two data breaches affecting 3 billion Yahoo users resulting in a \$350 million reduction in the purchase price of Verizon Communication's acquisition of Yahoo- bringing it down from \$4.8 billion to around \$4.48 billion.³ Another instance was that of a \$123 million GDPR fine being imposed on Marriott International owing to a data breach at Starwood Hotels and Resorts Inc. prior to its acquisition by Marriott.⁴

The Digital Personal Data Protection Act, 2023 ("**DPDP Act**") was passed by both the houses of the Parliament on August 2023,⁵ following a series of Draft DPDP Bills, and deliberations and stakeholder consultations by the Justice B.N. Srikrishna Committee spanning half a decade. Tracing its earliest genesis to the Supreme Court's nine Judge Bench decisions in *Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.*⁶ in 2017, which reaffirmed the right to privacy as a fundamental right under Article 21 of the Indian Constitution, the DPDP Act fulfils India's long-standing need for a robust and comprehensive data protection

¹ Digital Personal Data Protection Act, No. 22 of 2023, § 33(1) and The Schedule (India).

² Regulation 2016/679, art. 83(5), *General Data Protection Regulation*, 2016 O.J. (L 119) 1 (EU).

³ Nicole Perlroth, All 3 Billion Yahoo Accounts Were Affected by 2013 Attack, N.Y. TIMES (Oct. 3, 2017), <https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html>.

⁴ Kate O'Flaherty, Marriott Faces \$123 Million Fine for 2018 Mega-Breach, FORBES (July 9, 2019), <https://www.forbes.com/sites/kateoflahertyuk/2019/07/09/marriott-faces-gdpr-fine-of-123-million/>.

⁵ The Hindu Bureau, Digital Personal Data Protection Bill, 2023 Passes in Lok Sabha; Govt. Shrugs Off Exemptions, THE HINDU (Aug. 7, 2023), <https://www.thehindu.com/news/national/data-bill-passes-in-lok-sabha-govt-shrugs-off-exemptions/article67167943.ece>.

⁶ Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors, (2017) 10 SCC 1 (India).

legislation as opposed to the hitherto piecemeal and inadequate legal framework on this point- which essentially comprises Section 43A of the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 in addition to sector-specific data protection regulations like the RBI's Framework for Storage of Payments Systems Data applicable to the payments sector.

The disclosure and transfer of vast quantities of data, *inter alia*, from the target entity to the acquiring entity in an M&A transaction makes the target entity herein a data fiduciary under the DPDP Act and a data controller under the General Data Protection Regulation (“**GDPR**”) of the EU by virtue of processing and transferring digital personal data of data principals/subjects with a third party (acquiring entity), thereby attracting the applicability of provisions and obligations under the DPDP Act and GDPR, as the case may be.

This article evaluates and discerns the extant data protection frameworks governing M&A transactions in India and the EU, by undertaking a comparative analysis of the provisions and obligations applicable to M&A transactions (including exemptions applicable thereto) under India's DPDP Act, 2023 on one hand and the EU GDPR on the other. Given how the introduction of both these regulations and the resultant codification of data privacy obligations thereunder led to significant compliance costs for companies in their respective jurisdictions, this article also seeks to discern which of these two frameworks is more onerous for companies embarking on M&A transactions.

II. THE INDIAN FRAMEWORK

The DPDP Act, 2023 lays down only two permissible grounds for processing a data principal's personal data- processing for which a data principal has given their consent following Section 6, and that which is for certain legitimate uses.⁷ These 'legitimate uses' wherein data processing is permitted without obtaining the data principal's consent are enlisted under Section 7 of the Act and do not include M&A transactions within their ambit. However, there exists another set of exemptions by way of Section 17(1) under Chapter IV (Special Provisions) of the

⁷ Digital Personal Data Protection Act, No. 22 of 2023, § 7 (India).

Act whereby the situations listed therein are exempted from the application of provisions under Chapter II (*Obligations of a Data Fiduciary*) except Section 8(1) and (5) (*General obligations to comply with the Act and take reasonable security safeguards in respect of data possessed by a fiduciary*); Chapter III (*Rights and Duties of a Data Principal*); and Section 16 (*Protection and restrictions on transfer of personal data outside India*). In the list of exempted categories under this sub-section, clause (e) is reproduced as below:

“(e) the processing is necessary for a scheme of compromise or arrangement or merger or amalgamation of two or more companies or a reconstruction by way of demerger or otherwise of a company, or transfer of undertaking of one or more company to another company, or involving division of one or more companies, approved by a court or tribunal or other authority competent to do so by any law for the time being in force;”

Therefore, the DPDP Act, 2023 by virtue of Section 17(1)(e) carves out a specific exemption in favour of court-approved M&A transactions from obligations under the aforementioned provisions. Yet, what is pertinent to be noted is that this exemption is not available in all cases of transactions enlisted under Section 17(1)(e)- it is only applicable to those mergers/demergers/transfers of undertaking etc. which have been approved by a competent court/Tribunal or other authority.

Broadly, the provision refers to the schemes of compromise and arrangements, and mergers and amalgamations, governed by sections 230-232 of the Companies Act, 2013. Though not defined under the Companies Act, the schemes involve a compromise or arrangement between the company and its members or creditors.⁸ Similarly, mergers and amalgamations refer to the transfer of stakes between two or more companies and include demergers.⁹

The scope and coverage of this exemption for M&A transactions is something which has undergone variations across the various Draft DPDP Bills and the final Act. Under the Draft Personal Data Protection Bill, 2018, the permissible grounds

⁸ Companies Act, No. 18 of 2013, § 230 (India).

⁹ *Id.* §232.

for data processing included (in addition to processing by way of consent) processing for reasonable purposes under Section 17, which may include those related to, *inter alia*, mergers and acquisitions.¹⁰ The Personal Data Protection Bill, 2019 included a similar provision under Section 14(2)(c), as per which a reasonable purpose (for which data could be processed without consent) may include mergers and acquisitions. Then, the Digital Personal Data Protection Bill, 2022 brought in the concept of deemed consent, whereby a data principal is deemed to have given consent to the processing of their personal data in certain specified situations,¹¹ including M&As.¹² In contrast, the DPDP Bill, 2023 and subsequent Act have carved out an exception in favour of court-approved mergers, restructurings including by way of demergers, transfers of undertaking, etc., from all rights and obligations under Chapters II, III, and Section 16 barring Section 8(1), (5).¹³

Hence, the 2023 Bill and Act narrowed down the applicability of the M&A exemption to only court-approved M&A transactions relative to the previous DPDP Bills. At the same time, the exemption granted under the 2023 legislation, when applicable, is broader in its ambit than its predecessors in the sense that it extends to not only the requirement of consent but all other obligations accruing to a data fiduciary under the aforementioned Chapters and Sections of the Act. Further, it is worthwhile to note that the Draft Digital Personal Data Protection (DPDP) Rules, 2025 notified by the Ministry of Electronics and Information Technology (MeitY) on 3 January 2025 do not contain any rules or provisions clarifying or providing any guidance as to the ambit and implementation of the exemption in favor of M&A transactions under Section 17(1)(e).

III. M&A EXCEPTION UNDER THE EU GDPR

The GDPR lays down an extensive list of data protection principles governing the processing of personal data of data subjects, which must be followed

¹⁰ Draft Personal Data Protection Bill, 2018, § 17(2)(c) (India).

¹¹ Digital Personal Data Protection Bill, 2022, § 8 (India).

¹² *Id.* § 8(8)(b).

¹³ Digital Personal Data Protection Act, No. 22 of 2023, § 17(1)(e) (India).

mandatorily by anyone processing such data,¹⁴ with ‘personal data’¹⁵ and ‘processing’¹⁶ being defined broadly under the Regulation so as to cover anything and everything done with and to data that identifies a natural person (the data subject). The first and foremost of these principles is that of “lawfulness, fairness, and transparency.” Lawfulness is determined under Article 6, and would be upheld only if one of the six conditions thereunder are fulfilled, which means processing is lawful only if it is either based on the consent of the data subject, or if it is necessary for the performance of contract with the data subject or a legal obligation, and so on.¹⁷

But obtaining consent is impracticable in such situations, given time sensitivity, confidentiality, and onerous standards of consent. However, the GDPR does not carry any specific mention of its applicability (or the lack of it) to mergers and acquisitions of and between data controllers and data processors. Instead, data processing for the purposes of different stages of an M&A deal are brought under clause (f) of Article 6, which deems processing necessary if it is necessary for the purposes of the legitimate interests of the data controller. Simply speaking, when the consent of the data subject is lacking in respect of data processing during an M&A transaction, legitimate interests of the data controller come to the rescue to make the processing valid under the GDPR.

Invocation of the ‘legitimate interests’ basis requires fulfilment of a three-part test, as the language of the clause makes it clear. First is the Purpose Test, which entails considering whether the processing is for the purpose of pursuing a legitimate interest. A legitimate interest is lawful, specific, and not speculative.¹⁸ Examples include processing of employee or client data, prevention of fraud or

¹⁴ Regulation 2016/679, art. 5, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

¹⁵ *Id.* art. 4(1).

¹⁶ *Id.* art. 4(2).

¹⁷ Regulation 2016/679, art. 6, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

¹⁸ Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, EUR. COMM’N (Apr. 9, 2014), http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

direct marketing purposes, as stated in the GDPR itself.¹⁹ However, no exhaustive list can be prescribed and it is a situation-specific assessment in what qualifies as a legitimate interest.

Second is the Necessity Test, that is, whether the processing is necessary for achieving/furthering such legitimate interest. ‘Necessity’ is inclusive of reasonableness and proportionality.²⁰ So, it needs to be ascertained whether the data subject has a reasonable expectation that processing for the stated purpose may be done at the time and in the context of collection of their data.²¹ Further, the processing must be proportional to the purpose sought to be achieved, so if there is another reasonable way of attaining the same purpose that does not infringe on the data subject’s rights, then the proportionality test would fail. The European Commission’s Working Party on Data Protection has opined that ‘necessity’ is to be interpreted narrowly, thus increasing the threshold for legitimate interests.²²

Last is the Balancing Test, which means a balancing exercise must take place wherein the controller’s interests are balanced against that of the data subject, with the former shown to overpower the latter. This essentially means that sound justification is required when legitimate interests of the data controller are given priority over the interests and rights of the data subject. As the clause itself clarifies, such burden of proving precedence of business interests is higher when there is children’s data on the other scale. To demonstrate the balancing exercise, the *Google Spain*²³ case is paradigmatic. There, in finding a balance between the privacy of the data subject and the economic interest of the data controller, the

¹⁹ Regulation 2016/679, recital 47, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

²⁰ Information Commissioner’s Office, Legitimate Interests, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/legitimate-interests/#:~:text=This%20can%20be%20broken%20down,interests%20override%20the%20legitimate%20interest%3F> (last visited May 30, 2025).

²¹ Regulation 2016/679, recital 47, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

²² Article 29 Data Protection Working Party, *supra* note 18.

²³ Case C-131/12, *Google Spain SL & Google Inc. v. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González*, ECLI:EU:C:2014:317 (C.J.E.U.).

Court of Justice of the European Union looked at the gravity of the impact of processing on fundamental rights and freedoms of the data subject. It concluded that the data subject's right to obtain delisting of their bankruptcy status that relates to their private life, and not their public or professional persona, outweighs all other interests.²⁴

Thus, a bona fide M&A transaction falls within the scope of 'legitimate interests' as fulfilling all three requirements discussed above. Illustrative is the instance of two Greek insurance companies being granted an exemption from obtaining consent of their policyholders, clients and employees while executing a merger on the ground that it was necessary to fulfil a legitimate interest of the controller.²⁵

Data controllers and processors relying on the legitimate interest ground for lawful processing have still have to comply with other data protection principles and rights of data subjects, and only the requirement of consent is foregone. Purpose limitation, data minimization, transparency and accountability prescriptions, along with the rights of access, erasure and data security are to be observed.²⁶ This includes provisions as to third-country transfers of data, which has implications for reorganisation of the corporate structure of the data controller/processor with an entity that is not based in the EU. To be GDPR-compliant during such transactions, it must be ensured that the third country in which the other party(ies) is based follows data protection practices comparable to the EU, per Chapter V of the GDPR.

²⁴ *Id.* ¶ 80, 81.

²⁵ Nymity, Deciphering Legitimate Interests Under the GDPR: A Report Based on More Than 40 Cases From Practice, LEXOLOGY (Mar. 14, 2019), [https://www.lexology.com/library/detail.aspx?g=ba9dd603-2f73-4e42-a015-9fd130b2b724#:~:text=Providing%20Personal%20Data%20as%20Part%20of%20a%20Merger%20\(Greece\)&text=The%20DPA%20granted%20the%20exemption,controller%20or%20a%20thir%20party](https://www.lexology.com/library/detail.aspx?g=ba9dd603-2f73-4e42-a015-9fd130b2b724#:~:text=Providing%20Personal%20Data%20as%20Part%20of%20a%20Merger%20(Greece)&text=The%20DPA%20granted%20the%20exemption,controller%20or%20a%20thir%20party).

²⁶ Information Commissioner's Office, Due Diligence When Sharing Data Following Mergers and Acquisitions, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/ue-diligence/?q=upheld> (last visited May 30, 2025).

Additionally, data subjects have the unique right to object to data processing under-taken on the basis of legitimate interest. Once an objection has been raised by a data subject, processing can only proceed if the data controller is able to prove the existence of “compelling” legitimate interests satisfying the three-part test.²⁷ It has been noted that the standard of balancing is more onerous under Article 21 than in Article 6(1)(f), in that the mere existence of a legitimate interest is not sufficient; the legitimate interest must be compelling.²⁸ However, if objection is made against processing for direct marketing purposes, then processing must halt notwithstanding any justification.²⁹

The so-called merger exemption under the GDPR would only cover data processing during and related to the merger, and the data controller would not be absolved of any actual historic or upcoming breaches, including by third parties. For instance, Marriott was slapped with GDPR fines for security flaws in Starwood’s reservation system that pre-existed the former’s acquisition of the latter.³⁰

It must also be noted that the GDPR has wide extra-territorial application in that it governs any processing that is either done by a business situated in the European Union or any business that processes the data of subjects who are citizens of the EU for the purpose of offering them any goods or services, or for monitoring their behaviours.³¹ The implication is that the threshold of legitimacy of interests as well as fulfilment of other data protection principles must be observed by businesses outside the EU as well.

IV. THE M&A EXEMPTION UNDER THE DPDP ACT: WHOM DOES IT REALLY BENEFIT?

An analysis of the M&A exemption enshrined under Article 17(1)(e) of the

²⁷ Regulation 2016/679, art. 21(1), General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

²⁸ Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, EUR. COMM’N, (Oct.3, 2017), <https://ec.europa.eu/newsroom/article29/items/612053/en>.

²⁹ Regulation 2016/679, art. 21(3), General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

³⁰ Kate O’Flaherty, *supra* note 4.

³¹ Regulation 2016/679, art. 3, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

DPDP Act reveals that it suffers from two key infirmities. *Firstly*, since only court-approved M&As are beneficiaries of this exemption, data processing without the consent of the data principal during the due diligence stage is not covered within the scope of Section 17 since the need of it arises before approaching the competent authority to greenlight the transaction. However, it is widely accepted that due diligence is an inevitable and indispensable stage of any M&A transaction. It helps the acquirer not only assess the current regulatory compliance and mitigate the risk of potential regulatory sanctions due to an existing or future breach,³² but properly carried out due diligence further assists in the contract negotiation stage so that appropriate price and other conditions can be determined.³³ The scope and coverage of the present exemption hence does little to actually benefit companies that are parties to an M&A deal given that they are not entitled to any relaxation of the consent requirement at the crucial due diligence stage, and instead have to undertake the cumbersome task of obtaining the consent of all data principals whose personal data is possessed by the target entity, for the access to and processing of their data by the acquiring entity.

It is also unclear from the wording of the provision if approvals by the Securities and Exchange Board of India, Reserve Bank of India or Competition Commission of India are “approved mergers” under Section 17(1)(e), or only the M&A provisions under the Companies Act, 2013 are being referred to. Even if the former are covered, transactions such as the purchase of shares in a company under a private Share Purchase Agreement, leading to the sale of partial stake in the company or a 100% acquisition thereof, do not seem to be covered by the exemption as it currently stands. An example is a sale of a portion of an unlisted company to an unrelated entity within the country (particularly, when approval requirements are not attracted under any laws regulating M&As, namely,

³² Mark Steele, Philip Witchelo, Gail E. Crawford & Sian John, *GDPR Due Diligence in M&A*, FINANCIER WORLDWIDE (May 2018), <https://www.financierworldwide.com/gdpr-due-diligence-in-ma>.

³³ Lisa J. Sotto & Ryan P. Logan, *Navigating Privacy and Data Security Issues in M&A and Other Transactions*, HUNTON ANDREWS KURTH, BLOOMBERG LAW (2019), <https://www.huntonak.com/images/content/5/8/v2/58107/Navigating-Privacy-and-Data-Security-Issues>.

Competition law, Securities law, or Foreign Exchange law). This ambiguity arises on account of the fact that within the category of M&As, mergers and schemes under the Companies Act, 2013 requiring court approval are distinct from acquisitions by way of private or contractual arrangements falling outside the purview of the Companies Act such as an asset or share purchase, which do not require the approval of the court/NCLT to go through.³⁴ Hence, insofar as the exemption is only restricted to schemes of mergers or amalgamations “*approved by a court or tribunal or other authority competent to do so by any law for the time being in force*”,³⁵ it covers the former category but leaves out the latter from its ambit.

Secondly, the provision in question exempts court-approved M&A transactions from not only the requirement of consent of the data principal, but rather accords a complete exemption from all provisions under Chapters II, III, and Section 16 save Section 8(1) and (5). This firstly represents a huge ambiguity, insofar as Section 8(1) talks about the general obligation of a data fiduciary to comply “*with the provisions of this Act and rules made thereunder in respect of any processing undertaken by it*”. The exact scope of this obligation is hence unclear when a specific exemption has been granted from Chapters II and III under Section 17. Secondly, while the previous DPDP Bills incorporated an exemption in favour of M&As only to the extent of relaxing the consent requirement in such cases (as is also the case under the EU GDPR³⁶), the exemption under the 2023 Act clearly goes way beyond this and has an exceedingly wide amplitude. The rationale for exempting not only the consent requirement but also doing away with vital procedures and safeguards—such as in cases of processing data of children³⁷ and cross-border data transfers³⁸

³⁴ Ministry of Corporate Affairs, Report of the Expert Committee on Company Law—Chapter on Mergers and Acquisitions, <https://www.mca.gov.in/content/mca/global/en/data-and-reports/reports/other-reports/report-company-law/mergers-and-acquisitions.html> Parth Sugandhi, M&As: Share Acquisition by Private Arrangement—The Procedural Side, INST. OF CO. SECRETARIES OF INDIA (Aug. 2023), <https://www.icsi.edu/media/webmodules/CSJ/August/11.pdf>

³⁵ Digital Personal Data Protection Act, No. 22 of 2023, § 17(1)(e) (India).

³⁶ Regulation 2016/679, art. 6(1)(f), General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

³⁷ Digital Personal Data Protection Act, No. 22 of 2023, § 9 (India).

³⁸ *Id.* § 16.

as well as data principals' rights to correction, erasure,³⁹ and grievance redressal⁴⁰ is patently unclear.

Hence, while being seemingly M&A-friendly on the face of it by explicitly making an exemption for M&As, the framework under the DPDP Act, 2023 does not really benefit either of the two main stakeholders involved- consent requirements are still as onerous for data fiduciaries (parties to the M&A in this case) prior to court approval in case of court-approved schemes and altogether in case of all other arrangements, while key rights of data principal as to protection of their personal data and duties of fiduciaries in respect thereof have been inexplicably dispensed with.

Even the recently notified Draft Digital Personal Data Protection Rules, 2025, miss an opportunity to clarify and delineate the ambit of the M&A exemption or provide guidance as to its implementation in light of the clear ambiguities that exist in the wording of Section 17(1)(e). While being criticised as being 'too little too late' in the context of the larger discourse around the DPDP Act and its operationalization Rules seemingly do nothing to assuage the situation in relation to M&A transactions in particular.

V. THE SUGGESTED ALTERNATIVE: STRIKING A BALANCE

Notably, the following differences emerge between the Indian and EU M&A exceptions to data protection rules, including consent.

Firstly, unlike section 17 of the Indian DPDP Act, the GDPR does not specifically exempt M&A transactions from its compliance. Instead, the leeway is found within the "legitimate interests" basis of data processing, based on adjudicatory interpretation. The implication is that, the ground of "legitimate interests" is wider than that under the Indian framework so as to cover any and all data processing that can be said to be in the legitimate interests of the data fiduciary, although the invocation of the ground requires certain pre-requisites to be fulfilled including furnishing of a sound justification for the processing. On the

³⁹ *Id.* § 12.

⁴⁰ *Id.* § 13.

other hand, the DPDP Act lays down a very narrow exception that only refers to mergers approved by a court or tribunal.

Secondly, general applicability of the data protection provisions in case of M&As is excused in the Indian law that couches M&A transactions as a complete exemption. But since the GDPR states it as a ground of data processing, only the consent requirement is waived off under Article 6(1)(f) and the other safeguards that uphold data protection continue to be maintained.

In this regard, the Indian framework as applicable to M&A suffers from the twin shortcomings of being both more onerous and ambiguous than its EU counterpart. In order to remedy this position, various options emerge, which have been discussed in this section in order to ascertain which one would be the most suitable for India to adopt at this juncture.

The first alternative is the concept of deemed consent in certain situations like M&A transactions. Deemed consent refers to circumstances wherein personal data may be collected and processed without the knowledge and consent of the data principals owing to the impossibility/impracticality of obtaining consent in such cases, such as for medical, security, or law enforcement reasons. This can happen when there may not be enough time to obtain the requisite consent and/or seeking the consent of the person related to such data might defeat the purpose of collecting that information. To adopt this, the legislature need not look beyond its own 2022 Bill of the DPDP Act- which included M&As under the list of situations wherein the requirement to obtain consent was exempted by virtue of deemed consent,⁴¹ thereby extending the benefit to all M&As (and not just court-approved ones) whilst restricting the scope of the exemption to only relaxing the consent requirement. However, this concept of deemed consent was one that rightly received much criticism as part of the 2022 Bill and was hence dropped from the 2023 version of the Bill based on stakeholder consultations and feedback,⁴² given that it is principally problematic to deem data principals to have given their consent to the use of their personal data in cases when they have clearly

⁴¹ Digital Personal Data Protection Bill, 2022, § 8(8) (India).

⁴² Standing Committee on Communications and Information Technology, Forty-Eighth Report on Citizen's Data Security and Privacy (2023) 28.

not done so.

In light of this, the more appropriate route to take seems to be that of bringing M&A transactions under a reasonable purpose or legitimate uses clause. The difference between these two concepts is merely that of nomenclature- with the former being the one used in the previous iterations of the Personal Data Protection Bill prior to 2022⁴³ and the latter being the term employed in the 2023 Act;⁴⁴ and they both principally refer to the same concept- that of allowing data fiduciaries to bypass the requirement of obtaining the data principal's consent in situations (such as prevention and detection of unlawful activities) where it would be impossible or impracticable to do so,⁴⁵ as opposed to deeming data principals to have given their consent in such cases.

This being the case, the next question that arises is regarding the scope and ambit of such an exemption in favour of reasonable purposes/legitimate uses. One way to go would obviously be that of the EU GDPR, which makes data processing without consent lawful in cases where such processing is necessary for the legitimate interests pursued by the controller,⁴⁶ including M&A schemes⁴⁷- subject to fulfilment of a three-part test of purpose,⁴⁸ necessity,⁴⁹ and balancing between the interests of the data controller and subject. However, allowing processing without consent for such legitimate uses without providing an exhaustive list of what such uses include or prescribing standards to ensure uniformity in application may provide too broad a ground for bringing anything and everything under them, possible conflicts of interest, and use of excessive discretion and subjectivity in the case-by-case assessment that this would entail.⁵⁰

⁴³ Personal Data Protection Bill, 2019, § 14(2)(c) (India).

⁴⁴ Digital Personal Data Protection Act, No. 22 of 2023, § 7 (India).

⁴⁵ Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Report on A Free and Fair Digital Economy—Protecting Privacy, Empowering Indians (2018) 117.

⁴⁶ Regulation 2016/679, art. 6(1)(f), General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

⁴⁷ Nymity, *supra* note 24.

⁴⁸ Article 29 Data Protection Working Party, *supra* note 18.

⁴⁹ Information Commissioner's Office, *supra* note 20.

⁵⁰ Paolo Balboni et al., Legitimate Interest of the Data Controller New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection, 3(4) Int'l Data Privacy L. 251 (2013).

This was a concern rightly flagged by the Committee of Experts on a Data Protection Framework for India chaired by Justice B.N. Srikrishna, in its report on ‘A Free and Fair Digital Economy- Protecting Privacy, Empowering Indians’.⁵¹ Instead, the said report suggests an appropriate middle ground that ought to be adopted as far as this exemption is concerned- one whose ambit is circumscribed to the extent of allowing only a definite set of whitelisted activities like prevention and detection of unlawful activity and M&As to be entitled to this exemption from the consent requirement, and subject to procedural safeguards like giving of notice to the data principal if and when their data is being processed for such purposes without their consent.⁵²

Such a framework would achieve the best possible balance between the interests of the data fiduciaries on one hand and the vital rights of data principals on the other insofar as it accords a relaxation in favour of the former in case of M&As to suit the commercial and practical exigencies of such transactions, whilst firmly safeguarding the rights of the latter. This can be fitted into the existing framework of the DPDP Act, 2023 by merely moving M&As as a ground for exemption from Section 17 to Section 7 so as to bring them under the ‘legitimate uses’ wherein processing of personal data may be undertaken without consent under the Act. It is categorically suggested herein that in order to address the problems with the M&A exemption in its present form, the exemption being talked of be extended to all M&A schemes and transactions as opposed to only those under the Companies Act or requiring court approval, and in line with the aforesaid discussion, be accompanied by safeguards like data principals being adequately notified of any processing of their personal data pursuant to it.

Perhaps, in order to further strengthen the protection in favour of data principals’ rights, India would also do well to take a cue from the EU GDPR framework by giving data principals the right to object⁵³ to the processing of their personal data pursuant to such an exemption, which would automatically trigger the requirement for the data fiduciary to satisfy a much higher threshold and

⁵¹ Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *supra* note 44, at 118.

⁵² *Id.*

⁵³ Regulation 2016/679, art. 21, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

prove, in addition to mere coverage under the statutory exemption, a compelling interest for processing the principal's data without their consent which outweighs the interests and concerns of the data principal that are herein involved. This suggestion becomes relevant in light of the fact that while the DPDP Act, 2023 otherwise allows data principals to withdraw their consent to the processing of their personal data,⁵⁴ processing for legitimate uses without obtaining consent pursuant to Section 7 does not contain such a provision for the data principal to withdraw consent or essentially stop such processing of their data by a data fiduciary if they so wish.

Another deficient aspect of the DPDP Act that becomes relevant to a discussion on data protection during M&A transactions, arises out of Section 16 of the Act, which essentially permits cross-border transfers of data to all countries barring those to whom transfer of data is restricted vide notification by the Central Government.⁵⁵ Where either party in an M&A transaction may be situated abroad, free flow of personal data to such foreign entities gives too broad a scope for violating the essential data protection principles enshrined in the Act. While the GDPR standard of comparable data protection practices⁵⁶ may not work, given the shortfalls in India's own data protection provisions, the exemption for cross-border data flows herein (and specifically in respect of cross-border M&A transactions) should be withdrawn and such M&As should be subject to the same rules and requirements as a local M&A transaction.

VI. CONCLUSION

While much has been said and will be said regarding how the new data protection framework under the DPDP Act, 2023 is going to play out vis a vis different stakeholders like data fiduciaries (merging entities in case of M&A transactions) and data principals, the foregoing analysis reveals that particularly as regards M&A transactions, the provisions and exemption contained therein do little to benefit any of the stakeholders. That said, it has also been pointed out how even the EU GDPR framework may not be a perfect fit for India to directly

⁵⁴ Digital Personal Data Protection Act, No. 22 of 2023, §§ 5(2)(b), 6(4) (India).

⁵⁵ *Id.* § 16(1).

⁵⁶ Regulation 2016/679, ch. V, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

adopt given the wide ambit it accords for such an exemption and the resultant scope for subjectivity and misuse. It is therefore in light of this that the authors have suggested an alternate route that marries together the best practices and aspects of these frameworks in the interest of striking the best possible balance between the rights and interests of all stakeholders involved (primarily data principals and fiduciaries)- by exempting all M&A transactions (and not merely ones requiring court approval) from only the consent requirement herein by bringing them under the 'legitimate uses' for which data processing can be undertaken without the data principal's consent, subject to procedural safeguards like notifying the data principal of such processing and giving them the right to object to the same.