CROSS BORDER DATA TRANSFERS UNDER THE DPDP ACT AND THEIR STRUCTURAL IMPACT ON INDIAN M&A TRANSACTIONS

Vansh Chouhan & Khushi Tiwari, B.A.LL.B. (Hons.), Government New Law College, Indore[1]

ABSTRACT

The increasing indoctrination of evolving business on private and personal data has reconstructed the prospect of mergers and acquisitions. In India this modification corresponds with enforcement of Digital personal data protection Act, 2023, this statutory legislation has revised the regulation of how companies should assemble, process, store, and forward personal data. As cross border M&A keeps on enhancing, the DPDP Act has increased adherence barriers along with implications of structure, for both foreign acquires and Indian targets. This paper examines the pragmatic repercussions of the DPDP Act on deal structuring, due arduousness, estimation, risk determination and post-merger integration. The paper contends that data security is no longer an acentric compliance check but a pivotal pillar of transaction strategy. The perusal draws from comparative international practice, regulating trend, and emerging description to introduce a framework that lawyers, deal makers, and policymakers can rest on. Lastly the paper elicits by presenting suggestions for apparent guidance for regulation, safeguards for contracts, and industry practices that can aid smoother cross border transactions while maintaining privacy rights.

[1] B.A.LL. B (Hons.), Government New Law College, Indore

I. INTRODUCTION

The cross-border mergers and acquisitions is a well-known significant route through which global investment gets introduced in India. Some of the rapidly enhancing targets of foreign buyers and investors are Indian digital platforms, fintech companies, technology services providers, healthcare firms and retail enterprises. In all the above businesses, private and personal data establishes a peripheral asset, information of customers, including history of transaction, demeanour insights, health records, data of employees etc, as a culmination, personal data is now inseparable from the commercial value of enterprises.

In earlier times, the law for data protection of India was focused on Information technology Act, 2000[2] and its subservient rules. These rules were less in scope, fragile in enforcement and were deprived of detailed liabilities. As the Digital personal data protection Act, 2023[3] came in India has evolved with the modern approach of framework that is based on rights and provides guidelines for acquiring and transferring personal data. This is the very first approach where cross border transfers, of personal data are controlled explicitly, penalties as liability are substantial with a very adamant compliance obligation.

This growth has major consequences for cross border M&A transactions. Data protection matter now impacts almost each and every stage of the transactions, starting from initial negotiations and moving towards due diligence, estimation , structure of deal, documentation of transactions, lastly post-merger-integration, whenever any buyer acquires the Indian company, they must evaluate what data the target holds, storage criteria, consensual parameters, the transfer of data outside India In a legal way, and what peril may arise after the acquisition process is executed.

This paper thrives into all the issues with profoundness. It contends that the DPDP Act will reshape Indian M&A practice in the same manner the GDPR has restructured European corporate transactions.[4] It puts forth the areas that still needs further guidelines, to alter the ambiguities that can slow down investments and deals or reduce foreign investment.

II. THE DPDP PROVISIONS RELEVANT TO CROSS BORDER M&A

India's Digital personal data protection Act, 2023 changes the way for companies to collect,

[2] Information Technology Act, No. 21 of 2000 (India).
[3] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[4] Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

use, store and transfer personal data. The application of the Act is wide across the industries, some significant provisions become especially important as per involvement of foreign buyer, foreign patent company, or the activities of data processing across India. This section elaborates these provisions in a simple and pragmatic way, highlighting how they influence mergers and acquisitions instead of presenting a technical description on every section of law.

1. Significant data fiduciaries (SDFs) and normal data fiduciaries- The very heart of DPDP Act circumscribes in the concept of data fiduciary. In a simple language Data fiduciary refers to any organization that settles why and in what way personal data will be processed. The definition provided is very wide and extends to almost every evolving modern business, insurance providers, healthcare companies, app developers, and e-commerce platforms to banks. Whenever the foreign company analyses an Indian target for acquisition, evaluating its status as a data fiduciary becomes the very initial significant step. It if comes out that target contains a large volume of personal data or deals with sensitive categories including financial, biometric, health, or minors data it may be referred by the government as a Significant data fiduciary (SDF).[5] The SDFs are governed under the parameters of mandatory data protection impact assessments, regular audits, appointment of data protection officers based in India including higher surveillance and reporting standards.[6] The governance and distinction of SDFs makes a huge difference. A buyer must comply with the obligations of SDFs as they directly affect compliance costs, staffing needs, internal restructuring and long term based operational planning. A SDF target company may also face higher scrutiny as per regulations, that can directly impact timelines of deal enhances the amount of information the buyer must review during performance of due diligence

2. Framework of Consent- The consent is the most pivotal element of DPDP Act and that should be proper and meaningful, the mandates the consent must be, free from any force or manipulation, should be specific, duly informed, not based on conditions pertaining to unrelated services meaning unconditional, and lastly it should be unambiguous that further elaborates it should be clear and not assumed automatically.[7] This becomes the core of M&A due diligence. The problem persists where many Indian companies, especially start-ups, that scaled quickly, may have acquired personal data by furnishing vague consent notices or some privacy policies that are outdated. Some may not have taken user consent at all, or some have

[5] Digital Personal Data Protection Act § 10 (India).
[6] Digital Personal Data Protection Act § 11 (India).
[7] Digital Personal Data Protection Act § 6 (India).

executed their actions relying upon 'deemed consent' no longer acceptable. A foreign acquirer will be very vigilant about taking on such data when it was not acquired with lawful means. The acquirer may stand defeated in using it in such a way he always intended to. They may be compelled to alter the parts of the database or re obtain consent from millions of users, both of which is a very time consuming and sumptuous process.[8]

3. Rules of Cross Border Data Transfer- One of the most significant features of the DPDP Act is its approach to govern cross border data transfers. It is not like other drafts that India proposed for data protection laws, they introduced strict data localisation, the DPDP Act, 2023 adopts a more open model, which covers and puts emphasis on transfer of data outside India except to the countries that the government later notifies as restricted.[9] The approach of negative list brought by the government under which the restricted countries will be brought, appears to be very simple, but it creates uncertainty in pragmatic world because, there is no list of restricted countries published by the government, the list can be altered later, affecting long term business planning and most importantly companies have no idea what criteria the government will use to restrict transfers. Focusing on M&A, this uncertainty is a significant consideration for any deal.[10] The preference of buyers may differ, as to store data in a particular country, use a global data centre or integrate the target's data into their international systems. And as per DPDP Act, 2023 if the country becomes restricted later the whole business model will have to go through wide restructuring. The protection of buyers is preferred through warranties, indemnities, price adjustments, or by setting aside funds to handle future compliance costs.[11]

4. Penalties- When talking about the penalties under the DPDP Act they are deliberately strict. Depending on the way of violation, a company will have to face fines differing up to rupees 250 crore for each incident of noncompliance.[12] To mention the violations that can attract penalties include, failure of taking security measures, not reported data breaches, acquiring and processing data without valid consent, violation of cross border transfers rules most importantly

[8] Montagnani, Maria Lillà and Verstraete, Mark, What Makes Data Personal? (June 4, 2022). UC Davis Law Review, Vol. 56, No. 3, 2023 Forthcoming, Bocconi Legal Studies Research Paper No. 4128080, Available at SSRN: https://ssrn.com/abstract=4128080 or http://dx.doi.org/10.2139/ssrn.4128080

[9] Digital Personal Data Protection Act § 16 (India).

[10] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L. J. 677 (2015). Available at: https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2

[11] Christopher Kuner, Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law, 5 Int'l Data Privacy L. 235 (2015), Univ. of Cambridge Faculty of Law Research Paper No. 49/2015, https://ssrn.com/abstract=2644237.

[12] Digital Personal Data Protection Act § 33 (India).

not fulfilling duties of a data fiduciary or SDF. As per M&A, this means the buyer must profoundly calibrate whether the target has adhered with the DPDP Act in the past. If the target contains fragile data protection policies, the buyers may invite enormous financial liabilities. This can affect deal estimation, indemnity clauses negotiation, escrow holdbacks size, requirements of insurance, deciding integration timelines. Concisely, the penalties under the Act have introduced data compliance a key financial in the deals pertaining to M&A.

5. Data Processor Obligations- The reliance of Indian companies on third party vendors for cloud hosting, analytics, payroll, marketing, customer support and many other services is on a huge level, as per the DPDP Act, a data fiduciary is a responsible body for the actions of its data processors.[13] This straightaway establishes that if a vendor mishandles data, the liability falls on the main company not the vendor. And this aspect affects the M&A because the buyer will have to examine contracts of vendors, outsourcing arrangements, cloud service agreement, arrangements for data sharing with its affiliates, access control of third parties. If contracts do not include strong data protection clauses, the buyer can put forth renegotiation before closing, in some cases, in some situations the buyer can refuse to proceed unless there is full compliance of the vendor ecosystem.

6. Government Powers- The DPDP Act, 2023, furnishes wide powers to the central government, including restriction of data transfers to specific countries, seeking compliance reports from companies, issuing of direction and guidelines, designation of SDF's, along with surveillance of systemic privacy risks.[14] These powers can impact cross border M&A in distinct ways, such as if a target comes out to be under review or investigation, the buyer will face extreme risk, if a sector is referred as sensitive, essentials for regulation may be rigorous, and the directions of government in relation to data retention, breach reporting or security practices can inevitably affect integration planning and cost estimation. For foreign acquires, perception of the government's position becomes significant as India's regulatory compliance may affect not the legality but also the commercial feasibility of the deal.

III. THE ROLE OF PRIVATE AND PERSONAL DATA IN EVOLVING M&A

In most businesses, especially the operating digital platforms, very personal data is one of the foremost valuable assets. This part of paper delves into how such data influences deal making.

[13] Digital Personal Data Protection Act § 8 (India).
[14] Digital Personal Data Protection Act § 17 (India).

1. Data As Commercial Asset- As far as e-commerce companies are concerned about data to unlock consumer demeanour. For some Fintech firms, transactional and KYC data builds the strength and backbone of their business, for healthcare companies, the medical records are essential for delivery of services. The commercial value of such enterprises cannot be evaluated without assessing the core nature and quality of their data assets.

2. Data in Due Diligence- The earlier due diligence focused on financial accounts, risk of litigation, compliance of tax, and corporate records. On the other hand today, buyers must ask further additional questions and inquire about extended compliance likely, about the personal data that target holds, the measure of collecting such data whether lawful or not, what terms and conditions it holds for transferring it to the buyer's jurisdiction, if there exists any legacy breaches or complaints, whether the data assessing policies are satisfactory, lapses in any of these areas diminish the interest of buyers in the target.

3. International Comparisons- As per GDPR,[15] due diligence in data protection became a non-negotiable part of each and every governing European transaction.[16] India is deemed as leading towards it, the foreign buyers acquainted with GDPR level adherence will demand the same transparency from Indian targets.

4. Data Localisation Concerns- Referring to the DPDP Act as it does not impose rigorous data localisation, still India may restrict data transfers and processing to some jurisdictions, companies that deal with sensitive sectors like healthcare, financial services, defence tech may face heightened analysis.

IV. IMPACT OF DPDP ACT ON THE M&A LIFECYCLE

It is pertinent that the DPDP Act, 2023, impacts almost each and every stage of a cross-border M&A transaction. Earlier before 2023 the data protection was looked at only as compliance formality. Now, it substantially impacts and influences the feasibility, overall structure, cost and risk profile of a deal. The paper here aims to elaborate the influence in a stepwise manner, reaching to the four major phases of an M&A transaction, firstly pre-transaction analysis, due diligence, structuring of a deal, lastly post-merger integration.

1. Pre Transaction Stage- When the pre transaction stage is referred it means the buyer has to

[15] Regulation 2016/679, General Data Protection Regulation, art. 44 (EU); European Data Protection Board, Guidelines on Data Transfers under the GDPR (2021).
[16] Paul M. Schwartz, Global Data Privacy: The EU Way, 94 N.Y.U. L. Rev. 771 (2019), https://ssrn.com/abstract=3468554.

form very first impressions about the target company. As per DPDP Act, this stage becomes more emphasized and comprehensive because the buyer must get the target's data ecosystem.

Firstly, there comes data mapping and understanding 'Data footprint', mostly foreign buyers now require a comprehensive profile of target's data ecosystem even earlier than signing a term sheet. This covers the kinds of personal data the company covers, including criteria of storage, transfer of data outside the country, access of vendors or partners to it, storage of old and unnecessary data. A company with lousy documentation, ambiguous data practices, or fragmented systems becomes less attractive, interest less just because the buyer can't properly evaluate risk of compliance. No buyer wants to fall in the trap of huge pecuniary or technical liabilities under DPDP Act, 2023 that even extends up to 250 crores.

Secondly, early assessment of cross border transfer feasibility, since the personal data can only be transferred to the countries that remain unrestricted, the buyer has to analyse about its operational model, the planning of buyer to store their data in a particular country, can get their operational model doomed as India might label the country as restricted and prohibit the further transfers to that country in future. To understand it better we can refer to some hypothetical instances such as, a U.S buyer may wonder, what if the U.S is restricted later, A Japanese company, may evaluate the safety of its global data centre locations, and most importantly A European acquirer must ensure DPDP rules align with GDPR obligations. Thus, the jurisdiction risks are no longer only theory based; they can directly affect the proceedings of a deal.

Thirdly, impact on preliminary valuation when the target company heavily depends on personal data such as Fintech firms, health platforms, or marketplace apps, the buyer must analyse the scope to which the data can legally be used after acquisition. In the situation where portions of data can't be transferred or used, the estimation gets impacted. Referring to an example, if 20% of the user base has invalid or illegal consent, that 20% of the data can be left in high and dry, and become unusable until the consent is regained with lawful means, this can majorly reduce the commercial value of the target company.

Fourthly, Strategic fit and operational feasibility, in traditional notions, the strategic fit emphasized on business synergies, after the DPDP Act, the buyer will have to ask about the compliance of global system with Indian data laws, the requirements of integration whether it invites major technical changes, will the data stay in India, whether the target will require new staff or expensive compliance upgrades all of such issues and inquiries will have to complied by the buyer, also this analysis impacts whether the buyer even proceeds to the due diligence

stage.

2. Due Diligence Stage- The data due diligence has become one of the most significant parts of the transaction, before it was just a small section in legal due diligence, today it has to be a separate effort that will involve data experts, cybersecurity specialists and external auditors.

Consent quality review: The buyer has to verify the process of collecting consent by the target, making users informed properly, existence of consent logs, documentation from older versions of apps, nature of consent whether bundled, vague or hidden. The use of improper consent practices by the target, may invite the need of refreshing consent from the scratch, which can be an expensive and unrealistic approach for the buyer. In practical implications where an app with 50 million or above users cannot pragmatically, require new consent from all the users without losing a large ratio of them.

Review of Data Processing Agreements and Vendor Contracts: Under the DPDP Act data fiduciaries are liable for data processors, which means while due diligence buyers have to deeply examine, agreements pertaining to cloud hosting, outsourcing contracts, marketing analytics tools, customer service platforms, and IT & cybersecurity vendors, in case such contracts do not contain data security clauses, the buyer faces huge risk. It impacts in such a way that buyers often demand these contracts to be renegotiated before closing or they diminish the purchase price.

Cybersecurity and Breach History: Here comes a critical issue that whether target has ever suffered any data breaches, and if yes then the buyer must get clarifications on the proper reporting process, management whether internal without any disclosure, what were the corrective measures of the company, criteria of informing affected users. Otherwise, the buyer has to face penalties for a breach that occurred, before acquisition but was not addressed properly, this turns the breach history an emphasizing point of negotiation.

Data Retention and Deletion Practices: Where many companies store the unnecessary data exceeding the maximum duration that is prescribed for it, under the Act keeping data longer than required is a violation, it is compulsion on buyers to check out existence of deletion policies, removal of old data, erasing of user accounts deleted by the customers. Inappropriate deletion may expose the buyer to further liability.

Employee data and internal records: The data of employees is also personal data, buyers have to review, systems of HR, processing of payroll, background verification records, medical

insurance data and CCTV footage, at the time of integration process this data may need to be processed to global HR systems, which will require additional consent or adhering safeguards.

3. Deal Structuring Stage- When the buyer becomes adequate with due diligence, the next stage comes of designing the structure of the deal, the DPDP Act has widely transformed the way of deal structuring and documentation.

Share Purchase vs. Asset purchase: When it comes to purchase of share, the legal entity does not change, therefore, earlier and existing consents, may remain valid if the entity's identity remains same without any alteration due to share purchase. On the other hand, under asset purchase, there comes significant change of buyer becoming the new controller, that requires, consent to be freshly taken, new privacy notices, new user agreements, that turns out to be very difficult, when the target has millions of users, that's why companies now prefer share purchases when heavy data businesses are indulged.

India Based SPVs (Special purpose Vehicles): It is upon the foreign buyers that they may create India based subsidiaries or SPVs, to store personal data locally amidst escalating other assets offshore, this minimises the infliction of legal burden of cross border transfers. Although it also aids when a buyer's home country may come under restrictions list of India under DPDP Act in future.

Indemnities, Warranties, and Escrows: As per the high penalties under the Act, buyers now require comprehensive warranties, such as: "lawful collection of companies personal data", "no occurrence of any breach in last 3 years", "compliance of all the vendors with DPDP essentials". If any of the information turns out to be fabricated or false, the buyer can demand and ask for compensation also the amounts of escrow money kept aside for danger and risk have been enhanced in heavy data dealing.

Conditions Precedent (CPs): Conditions Precedent often refers to the actions that seller must comply before the deal closes, such as privacy policy updating, consent regularisation, strengthened cybersecurity, renegotiation of vendors contracts, conduct of internal audits, when CPs are not finished, the chances are likely buyer walking away or delay the closing of deal.

4. Post Merger Integration Stage- Closing of the acquisition process invites integration of data systems across borders which is one of the most fragile, and time-consuming actions.

Constraints in Data Migration: When the buyer's global systems are therefore situated in a

country that comes under restricted lists of India at a later stage, migration of the data falls under the liability of unlawful process. In that case companies may have to create a storage system that is separate and belongs to only India, splitting of user accounts and regional data, and maintenance of dual infrastructures, that enhances the costs of operation.

Aligning Privacy Policies and interfaces of user: As the deal concludes, buyer has to integrate the notice pertaining to target's privacy into the global privacy regulations, the interfaces of users may be required for redesigning and collection of compliant consent, and the teams of helpdesk have to be provided training on handling user requests under the act, all these efforts need time, expenses, and technical compliance.

Harmonization of Security Standards: Most of the foreign companies often have typical, cybersecurity systems, they must upgrade and evolve the target's systems so that it can stand at the footing of global standards, which consists, firewalls updating, old data encryption, internal access limitations, upgraded cloud infrastructure, and checks pertaining to vulnerability, if all such requirements are not met and complied most likely they will result in penalties.

Historical Data Handling: One stashed challenge is old and traditional data collected years ago that too with due and proper consent. It is the responsibility of the buyer to determine whether the old data should be deleted, requirement of new consent, usefulness of that data, and inflicting restriction to access until clarifications of compliance are furnished. All these decisions straightaway impacts progress, marketing and extended long term business plans.

Managing Government Interaction: When the target belongs to the sensitive sector, the government may keep a check on compliance more deeply and the buyer must maintain audit reports, statements of compliance, notifications of breach, regulators required clarifications, the foreign companies involve Indian law firms to administer and manage this communication.

V. CASE STUDIES AND PRACTICAL SCENARIOS

As far as it is understood that India is in its initial stages of implementing and complying DPDP Act, there are not many public M&A cases showcasing how the law and rules of DPDP affected a deal. Although, to comprehend the real impact, it is helpful to use pragmatic scenarios on the several types of transactions happening in the Indian market. The instances are realistic and structured on the hurdles that companies face, but they are presented in a simplest language to depict how the DPDP Act can shape cross border M&A.

Scenario 1: where a U.S Technology Company Acquires, an Indian Fintech startup

A U.S based financial technology company, determined to acquire a rapidly growing Indian Fintech platform, that provides digital lending and online transactions. The point to emphasize is that most of the Indian startup comes directly from its customers database, spending structure and pattern, documentation of KYC, and credit score algorithm.

Key Issues:

● Problem of consent: The Indian based startups have collected most of its customers data before DPDP Act, most of the customers have forgotten about signing consent forms, and some of the consents are hidden inside long terms and conditions pages, this introduces risk because the buyer remains uncertain whether the data can be legally used after acquisition.

● Cross border data transfer: Even if U.S buyer today wants to store the data in global servers outside India, under the DPDP Act there is no guarantee that the US cannot come under the restriction clauses of India in future, this brings ambiguity and uncertainty for the buyer.

● Liability for Old Violations: Due to noncompliance of proper security practices by Indian startups, or even mishandling of such data in the past, can impose penalties on the new buyer extending up to 250 crores.

Impact On the Deal: Its effect can be seen as buyers demanding stronger warranties from the founders. Part of purchase price can be held in an escrow account, buyers can insist on a full data audit before deal closing, there can be reduction of valuation amount because of uncertainty around consent and cross border transfers. All these scenarios show how the DPDP Act impacts pricing and structure.

Scenario 2: A European healthcare company merges with an Indian hospital chain

As it is well known the healthcare companies handle most sensitive personal data and under the DPDP Act the most sensitive health data must be processed with even more care and safety.

Key Issues:

● Storage of Data: When a buyer keeps patient records in Europe where GDPR applies that has restructured the transparency and transactions whereas the Indian hospitals keep them on local servers integrating the two distinct systems becomes harsh and difficult because both laws must be complied.

● Consent from parties: There comes the most significant hurdle when some of the patients did not furnish specific consent, for their data to be shared and processed outside the country.

● Data Retention: When the hospital retains the medical files of their patients, for many years, but the buyer wants to alter and delete older data to minimize risk, it is not easy to be performed as Indian law sometimes mandates the hospitals to store records for a minimum duration, and deletion of data before the prescribed time may encourage liability.

Impact on the deal: The buyer will have to create two distinct data systems: one in India and one in Europe, including post-merger integration that consumes longer duration and costs more, and insertion of indemnity clauses by the buyer to protect in case of past breaches by the hospital. These instances depict the rigorous method of merging companies from sectors with heavy data liabilities and obligations.

Scenario 3: A Japanese E commerce company Buys an Indian Retail platform

This is the simplest deal but contains hurdles and ambiguities as per compliance of the DPDP Act.

Key Issues:

● Vendor Contracts: The Indian companies rely on many external third-party vendors for packaging, delivery, marketing and cloud hosting, under the DPDP Act, the company is accountable for such vendors, The buyer must analyse each contract of vendors.

● Employee data: The buyer while moving employee records to a collaborative HR system in Japan, in later stages if Japan comes under the restriction implied by India as per DPDP Act, this could cause severe issues.

Impact on the deal: The buyer will have to renegotiate multiple distinct vendor Contracts, there will be need of additional consent from the employees just before transferring their data, the funds relating to upgradation compliance can be set aside.

VI. CHALLENGES, GAPS AND GREY AREAS OF DPDP ACT, 2023

Eventually the DPDP Act is huge growth towards data protection still there are several distinct issues that remain ambiguous. The vacuum affects cross border M&A and brings uncertainty for foreign buyers. Here we will thrive into the major hurdles elaborated in simple terms.

1) There are no clear restricted countries specifications yet, the Act establishes India can

prohibit data transfers to certain countries, but has not provided names of those. This major lapse introduces a risk barrier for cross border deals because an unrestricted country can fall into the domain of restrictions in future.

2) The Act does not contain any Standard Contractual Clauses (SCCs) yet, in an evolved country like Europe, companies aid through standard contractual clauses that is approved by the regulator to process and forward data safely, India is still deprived of any such model agreements. This creates ambiguity for companies that are confused about what "sufficient protection" means in a pragmatic view.

3) Also, India has no guidelines for valuation of data, where many companies depend heavily on personal data for their business model, it creates a grey area for the valuation of data during acquisition. There's no prescription of any norms when the data can't be lawfully transferred.

4) Uncertainty in the requirements of consent also exists as a major issue, if old primitive data was acquired with undue and poor consent, how far the customers shall be contacted again for re- gaining consent. For huge platforms this is not easy, it is rigorous, although this ambiguity impacts valuation and feasibility of deal.

5) There also exists conflicts with other laws, like many Indian laws affect cross border business activities, including, foreign exchange rules, Security and exchange board of India regulations, competition act, and some rules that are sector specific for telecom, banking and finance, insurance and healthcare. The DPDP Act itself does not provide explanation on interaction of these laws this can ultimately delay transactions and make the process of due diligence more complex.

6) Several Indian startups do not have advanced data protection systems, such acquisition targets lacking the compliance come under the liability. Which can impact estimation and demotivate investments.

VII. SUGGESTIONS FOR FLEXIBLE CROSS BORDER M&A UNDER THE DPDP Act 2023

To make cross border deals unrough along with protection of privacy, there is a strong need of apparent guidelines and strengthened practices for both government and the industries itself. To introduce smoother transactions the recommendations are as follows:

List of Restricted countries: This will aid the companies to plan long lasting operations and

neglect sudden prohibitions.

Standard contractual clauses: The country shall provide model clauses that can aid in data transfers, just like EU SCCs. This can minimise duration of negotiation and ambiguity of law.[17]

Transitional Period for Old data: Most of the companies have already collected major data before the enforcement of DPDP Act, that government shall prescribe "Grace Period" that will help companies in regularising consents rather than losing valuable data.

Guidelines for M&A Due diligence: SEBI, MCA must issue an advisory elaborating the essentials for companies to abide by while performing due diligence. This will ultimately standardize market practice.

Data Audits Before Transactions: There should be a norm of data protection audits just before the deal that will definitely minimize astonishment for both the parties.

Promote Training and Capacity Building: India should look forward towards organizing workshops and training sessions for the companies to get acquainted with the DPDP Act and their liabilities.

VIII. CONCLUSION

Cross border M&A is one of the most significant measures for enhancing economic and global growth for India. The country has become a huge digital economy; personal data of consumers forms a peripheral asset in business transactions. The enforcement of DPDP Act in India embarks a major alteration in how companies must manage the data.

This paper puts emphasis on the influence of DPDP Act in almost each and every stage of cross border M&A deal whether it is pre transaction, structural basis, due diligence and post-merger integration all of these processes have been impacted severely through the implication of the act. Foreign buyers must analyse about storage, consent, historic practices, risks after acquisition before coming to any estimation of deal. Indian targets will have to upgrade their database to remain in interest for foreign investors.

The DPDP Act introduces more stable and stringent privacy protection but also new hurdles just like every coin has two sides. The DPDP Act also contains positive and negative areas, the lack of clarity on specific issues of restricted countries, standard clauses and old data will slow

[17] Commission Implementing Decision (EU) 2021/914, Standard Contractual Clauses for International Data Transfers, 2021 O.J. (L 199) 31.

down deals. These hurdles shall be fixed through better guidelines, enhanced contract practices, and much better internal systems. Ultimately the law puts forth the Indian companies towards good governance and transparency. Once these practices fall into habitual perception, cross border M&A in India will definitely become more flexible and trustworthy. Filling the vacuum between regulation and flexibility, India can become a major global investment hub.