INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

"NAVIGATING DATA PRIVACY RISKS IN M&A TRANSACTIONS: A COMPARATIVE LEGAL ANALYSIS OF DUE DILIGENCE UNDER INDIAN AND GLOBAL FRAMEWORKS"

AUTHORED BY - SHARON MABEL JOY

ABSTRACT:

The increasing speed at which companies are taking part in mergers and acquisitions (M&A) in the digital economy poses questions with data protection and privacy, most notably with respect to the due diligence process. This paper examines the obligations and consequences, relating to data privacy, but concentrates on the Digital Personal Data Protection Act, 2023 (hereinafter, DPDPA, 2023) and relevant provisions of the Information Technology Act, 2000 under Indian law. This paper will also provide important consideration to key international regulatory frameworks including GDPR, CCPA and other statutes to examine the extent to which global standards now shape the cross-border due diligence processes of M&A transactions. The research has revealed significant areas of concern regarding India's present framework for M&A transactions, specifically in relation to consent, data-sharing activities, and the cross-border transfer of data relating to the M&A transaction. The research has also examined the data privacy-related risks attributable to non-compliance with the relevant regulations and reputational damage, and how these factors affect decision-making and influence the transactional process. Finally, the research applies a comparative law methodology to propose specific recommendations to improve India's data privacy due diligence processes to align with best international practices. This research contributes to the on-going narrative regarding various mechanisms for the harmonization of data protection standards in cross-border M&A transactions. This research also consolidates important findings into practical considerations for legal advisors, corporations and government representatives.

Keywords: *Merger & Acquisition, Data Protection, Due Diligence, Legal Framework, Digital Personal Data Protection Act.*

ISSN: 2582-6433

LITERATURE REVIEW:

1. Mahnoor Ali & Mujadad Jamil, Legal Challenges and ESG Due Diligence in Cross-Border Mergers and Acquisitions (M&A) in the US, SSRN (2025).[1]

The article "Legal Challenges and ESG Due Diligence in Cross-Border Mergers and Acquisitions (M&A) in the US" by Mahnoor Ali and Mujadad Jamil (2025) delves into the convergence of ESG issues and legal intricacies in cross-border M&A transactions with the U.S. The study aims to explore the integration of ESG considerations in legal due diligence, with a focus on issues of regulatory, contractual, and governance nature. Through doctrinal legal scholarship and qualitative case study investigation, authors investigate the role of ESG in deal structuring and post-merger success. Key findings point to increasingly salient ESG issues in valuation, risk, and compliance, in spite of ongoing data gaps and regulatory fragmentation. Variables are ESG metrics, legal risks, compliance obligations, and transaction structures, influencing a conceptual framework to connect ESG diligence with M&A success. The article concludes there is a gap in ESG integration model standardization and there is a need for a harmonized legal-ESG diligence model in cross-border transactions.

2. Pranay Singha, Regulatory and Legal Challenges in Cross-Border Mergers and Acquisitions, Vol. 9 Issue 5 J. Legal Stud. & Res. 88 (Sept. 29, 2023).[2]

The research paper "Regulatory and Legal Challenges in Cross-Border Mergers and Acquisitions" authored by Pranay Singha and presented in the Journal of Legal Studies and Research (Vol. 9, Issue 5, 2023) is a critical evaluation of the intricate international M&A transaction global regulatory regime. The primary aim of the study is to determine the legal, tax, antitrust, environmental, and labor law challenges faced by companies when opting for cross-border mergers. Using a doctrinal research methodology supported by comparative case studies, the paper identifies such key variables as regulatory approval procedures, intellectual property protection, competition levels, and jurisdictional legal risks. The findings suggest the imperative of coordinated law at an early stage, compliance planning in strategy, and holistic due diligence as the key to deal efficiency. The study establishes that the dispersed nature of cross-border regulatory arrangements tends to slow down transactions and enhance legal uncertainty. It recognizes a gap in research where there is no single global regulatory model and offers a systematic framework connecting regulatory readiness to effective post-merger

[1] Mahnoor Ali & Mujadad Jamil, Legal Challenges and ESG Due Diligence in Cross-Border Mergers and Acquisitions (M&A) in the United States (SSRN Working Paper, 2025), https://papers.ssrn.com
[2] Pranay Singha, Regulatory and Legal Challenges in Cross-Border Mergers and Acquisitions, 9 J. Legal Stud. & Res. 88 (Sept. 29, 2023), https://thelawbrigade.com

ISSN: 2582-6433

integration.

3. Dr. Hanuman Sahai Kumawat, Challenges and Opportunities in Conducting Due Diligence in India: A Sectoral Analysis, Vol. VIII Issue III NBMF (July–Sept. 2023)[3]

Dr. Hanuman Sahai Kumawat's 2023 paper, published in NBMF (Vol. VIII, Issue III), discusses the challenges and prospects in sectoral due diligence practice in India. It seeks to identify regulatory, financial, legal, and operational issues in healthcare, manufacturing, IT, and finance sectors. Using a doctrinal and comparative case-study approach, the paper analyzes factors such as sectoral compliance standards, levels of transparency, and risk management practices. Key results identify sectoral disparities in data availability, regulatory overhang, and increasing use of digital tools to simplify diligence. The research concludes that despite challenges particularly with red tape and sector regulations adopting technology and specialist advisory services presents substantial opportunity. It identifies research lacuna in cross-sector benchmarking and urges a harmonized sector adaptive due diligence framework for increased efficiency and deal quality.

4. Anita Åkerman, Cultural Compatibility in Cross-Border M&A: Addressing the Gaps in Due Diligence for Successful Integration (2025) (unpublished master's thesis, Theseus, Finland).[4]

Anita Åkerman's study examines why cross-border M&A ignores cultural due diligence despite its important role in successful post-merger integration. The research aims to assess cultural fit, identify common integration gaps, and propose applicable instruments to incorporate culture analysis into due diligence. Using a mixed-methods approach, the author interviewed M&A practitioners and employee questionnaires of acquired companies to obtain both expert opinion and employee perspectives. Critical variables are rate of evaluation, availability of instruments for cultural analysis, attribution of responsibility, and performance of integration. Results indicate that regular cultural assessment is uncommon, constrained by timing, lack of tools, and undefined responsibility but that early cultural due diligence can forestall many problems post-deal. The research concludes that the use of simple cultural assessment instruments in due diligence increases integration success and suggests organizations implement formalized cultural reviews as best practice.

[3] Hanuman Sahai Kumawat, Challenges and Opportunities in Conducting Due Diligence in India: A Sectoral Analysis, VIII NBMF, Issue III (July–Sept. 2023), https://bnwjournal.com

[4] Anita Åkerman, Cultural Compatibility in Cross-Border M&A: Addressing the Gaps in Due Diligence for Successful Integration (Master's Thesis, Theseus, Finland, 2025), https://www.theseus.fi

ISSN: 2582-6433

5. Chokri Kooli & Melanie Lock Son, Impact of COVID-19 on Mergers, Acquisitions & Corporate Restructurings, 1 Businesses (MDPI) 102 (Aug. 16, 2021).[5]

The paper "Impact of COVID-19 on Mergers, Acquisitions & Corporate Restructurings" by Chokri Kooli and Melanie Lock Son (2021) gives a contemporary analysis of the manner in which the pandemic shifted global M&A strategy, specifically in terms of driving digital due diligence and remote integration processes. Although the paper is on its core most concerned with economic and operating implications, indirectly it does contribute to the increasing significance of data privacy by discussing how virtual data rooms, remote transaction making, and greater monitoring of health-related worker information have enhanced the intricacy of compliance environments. These trends emphasize the urgent need to rethink legal requirements around data protection in M&A, particularly in a cross-border digital landscape. While the research is not specifically focused on privacy law, its conclusions set out the environment in which data privacy has become an increased concern under the rubric of due diligence. This makes it reasonable to examine how frameworks such as India's DPDP Act and GDPR converge with each other, given that legacy legal paradigms of M&A due diligence have not yet kept pace with pandemic-driven digitisation. The article helps to establish the imperative and significance of your subject matter for ongoing research on legal privacy obligations in the digitisation of M&A landscapes.

6. Yuan Sun, Data Security and M&A (M.Phil. thesis, Lingnan Univ. Aug. 23, 2021).[6]

Yuan Sun's MPhil thesis "Data Security and M&A" (awarded August 23, 2021, Lingnan University) examines if data security is a driving force in M&A deals during the big data era. It seeks to determine how state-level data breach notification (DBN) statutes affect the intensity and probability of M&A activity in U.S. states. Through the use of an empirical economics methodology applying staggered DBN law adoption and industry-level cyber-risk variation the research analyzes pre- and post-adoption target acquisition rates. Variables are DBN law status, M&A frequency and volume, and industry cyber-risk, and methodology utilizes state-industry-year panel data. Critical results indicate that DBN implementation raises M&A activity in states where acquirers already have breach laws (lessening data lemons) but lowers it where acquirers are based in states that lack such laws (because there are higher breach-related expenses). The research concludes that information security and improved cybersecurity models are important

[5] Chokri Kooli & Melanie Lock Son, Impact of COVID-19 on Mergers, Acquisitions & Corporate Restructurings, 1 Businesses (MDPI) 102 (2021), https://www.mdpi.com/journal/businesses
[6] Yuan Sun, Data Security and Mergers and Acquisitions (M.Phil. Thesis, Lingnan Univ., Aug. 23, 2021), https://commons.ln.edu.hk

ISSN: 2582-6433

drivers of M&A conduct, and it presents a research gap around the way legal frameworks of privacy influence deal structure urging further investigation of how data protection regimes should be included in M&A due diligence.

7. Emil Hansson, Data Protection Considerations in Pre-Merger Process: Due Diligence and Merger Assessment (unpublished M.A. thesis, Lund Univ. 2024).[7]

Emil Hansson's thesis "Data Protection Considerations in Pre-Merger Process: Due Diligence and Merger Assessment" (2024, Lund University) offers a technical legal analysis of the impact of the GDPR on data protection needs during the M&A due diligence process in the EU context. The study identifies that while GDPR demands stringent processing of personal information in pre-merger notifications, merger evaluations under competition law barely involve privacy concerns except where there is a question of market dominance. With a doctrinal analysis, Hansson critically discusses regulatory overlap and fragmentation between data protection and competition regimes. Key findings are that data protection is addressed as a parallel compliance matter instead of a key evaluative consideration for merger sanction. Convergence regulation and more transparent legal rules on data treatment in transactions are necessitated by the thesis. Its application to this research is offering an EU benchmark for incorporating data privacy within M&A due diligence that permits comparative legal review with India's DPDP Act and global standards such as GDPR.Key findings are that data protection is being dealt with as a parallel compliance issue rather than a key consideration for review of mergers. Regulatory harmonization and even more transparent legal prescriptions on data handling in transactions are demanded by the thesis. Its use in this research is offering a European benchmark for incorporating data privacy into M&A due diligence, thus enabling the comparative legal examination to be possible with India's DPDP Act and global standards such as GDPR.

8. James A. Sherer, Taylor M. Hoffman & Eugenio E. Ortiz, Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, E-Discovery, and Information Governance into Due Diligence Practices, 21 Rich. J.L. & Tech. 5 (2015).[8]

James A. Sherer, Taylor M. Hoffman &Eugenio E. Ortiz's "Merger and Acquisition Due

[7] Emil Hansson, Data Protection Considerations in the Pre-Merger Process: Due Diligence and Merger Assessment (M.A. Thesis, Lund Univ., 2024), https://lup.lub.lu.se.
[8] James A. Sherer, Taylor M. Hoffman & Eugenio E. Ortiz, Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, E-Discovery, and Information Governance into Due Diligence Practices, 21 Rich. J.L. & Tech. 5 (2015), https://jolt.richmond.edu

ISSN: 2582-6433

Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, E Discovery, and Information Governance into Due Diligence Practices" (2015, Richmond J.L. &Tech 21(2)) proposes a structured framework that brings together data privacy, cybersecurity, e discovery, and information governance in M&A due diligence.The objective is to bring data management concerns to the same strategic level as legal and financial diligence. Through doctrinal analysis, the authors point to five verticals DP, IS, IG, e-Discovery, and deal documentation as critical variables. Their model highlights nascent dangers of digital deals and provides practical checklists to evaluate information governance, encryption, access controls, and data breach history. Findings support that sound data-centric due diligence can dramatically lower cybersecurity and compliance exposures. The research concludes that M&A procedures need to transform to address data-related requirements systematically and offers a benchmark model currently underexploited across jurisdictions reflecting a gap for comparative studies of Indian and foreign privacy regimes.

9. Dr. Parineeta Goswami, Comparative Analysis of Acquisition Agreements Across USA and India (Dec. 20, 2024).[9]

Dr. Parineeta Goswami's paper "Comparative Analysis of Acquisition Agreements Across USA and India" (2024, UPES) provides a valuable cross-jurisdictional assessment of how acquisition agreements are structured in India and the U.S., with specific emphasis on contractual elements such as representations, warranties, indemnities, and liability allocation. While not solely about data privacy, the research provides key insights into the allocation of legal risk ranging from compliance risks to disclosure risks between parties. This is directly applicable to the current study, as data protection responsibilities increasingly become part of the contractual framework in cross-border M&A. By identifying gaps in standardized clauses and negotiation practices, particularly around regulatory and compliance risks, Goswami's work underscores the need to incorporate specific data privacy provisions within acquisition agreements. Her comparative approach also lays the groundwork for evaluating how Indian and U.S frameworks differ in addressing emerging obligations under data protection regimes such as the DPDP Act and CCPA. This aligns with the general objective of this dissertation: to create a privacy-oriented legal due diligence framework tailored to realities of cross-border deals.

[9] Parineeta Goswami, Comparative Analysis of Acquisition Agreements Across the United States and India (Dec. 20, 2024), https://papers.ssrn.com.

ISSN: 2582-6433

10. Mahnoor Ali & Mujadad Jamil, Legal Challenges and ESG Due Diligence in Cross-Border Mergers and Acquisitions (M&A) in the US, 3 Rev. L. & Freedom 1 (2023).[10]

Mahnoor Ali and Mujadad Jamil's paper "Legal Challenges and ESG Due Diligence in Cross Border Mergers and Acquisitions (M&A) in the US" (2025) critically examines the legally intertwined and ESG complexities in U.S. cross-border M&A transactions. The authors employ a doctrinal and qualitative case-study methodology to examine regulatory overlap—securities, antitrust, environmental law, and national security reviews and the role of ESG factors that now prevail valuation, structuring, and post-merger compliance. Primary findings identify that ESG diligence extensively drives representations, warranties, indemnities, and completion conditions, as well as major obstacles posed by fragmented regulatory frameworks and disparate data standards. The research concludes that effective cross-border M&A requires an integrated legal ESG due diligence, but finds a research void in standardized ESG–legal integration models. This highlights the need for an integrated framework similar to your data privacy due diligence model balancing regulatory, ESG, and legal aspects across geographies.

INTRODUCTION:

Mergers and acquisitions (M&A) have become a crucial tactic for businesses seeking to expand their reach and obtain a competitive edge in the ever evolving global economy of today. The stakes are greater than ever as companies expand internationally to reach new markets, and the complications increase.[11] The buying, selling, splitting, and merging of various businesses and related entities is referred to as mergers and acquisitions (M&A) in the context of corporate strategy, corporate finance, and management. Partnerships, governmental organizations, the enforcement of antitrust and competition laws, and the channels via which companies are acquired and divested are examples of entities. Although M&A is a very broad phrase that occasionally covers more important subjects like privatizations, shareholder pressure on management, and businesses that deal in stocks, it cannot consistently replace a significant number of employment. Acquisitions and mergers are a crucial and significant aspect of business, particularly when it comes to gaining expansion. M&A activity increases in prominence in such intense battles for expanding enterprises.[12] Mergers and acquisitions

[10] Mahnoor Ali & Mujadad Jamil, Legal Challenges and ESG Due Diligence in Cross-Border Mergers and Acquisitions (M&A) in the United States, 3 Rev. L. & Freedom 1 (2023), https://revlfreedom.org
[11] Mahnoor Ali & Mujadad Jamil, Legal Challenges and ESG Due Diligence in Cross-Border Mergers and Acquisitions (M&A) in the U.S., SSRN Working Paper No. 5330630 (2025), https://ssrn.com/abstract=5330630
[12] Rashid Khan & Muntazir Khan, Legal Challenges of Mergers and Acquisitions in Global Markets, Law Res. J., 25–33 (2025), https://lawresearchreview.com/index.php/Journal/index

ISSN: 2582-6433

(M&As) involve a number of factors, and due diligence is the process of planning a commercial deal by researching the target company. A due diligence procedure looks for integration potential in the targeted organization. Nonetheless, the focus of due diligence is typically on analyzing the target company's assets, competencies, and financial situation. Cultural factors are rarely taken into account during a due diligence procedure.[13]

Data privacy becomes a substantial consideration when a company is involved in a merger or acquisition, as any merger or acquisition involves the transfer of vast amounts of personal information and other sensitive data. In India, the new Digital Personal Data Protection Act, 2023 proposes to provide a legal framework for lawful data processing, consent for data processing and accountability, especially in a corporate transaction. The Act creates compliance obligations for data fiduciaries to take appropriate care of personal information in the due diligence stage and as part of a business acquisition. These obligations related to accountability and compliance show India's desire to ensure data privacy while also enhancing business growth and cross border investment into India.[14]

Alternatively, in the United States, a sectoral and state based approach is taken. Laws such as the California Consumer Privacy Act (CCPA) grants individuals rights to their data- like to access it, deleted it, or opt out of its sale- while requiring obligations for businesses to act with transparency and accountability.[15] While India's more nationalized approach takes a more encompassing nationwide approach, in the U.S. compliance can vary greatly from state to state and sector to sector which creates a more complicated compliance structure for M&A transactions. The United Kingdom, on the other hand, has the UK General Data Protection Regulation (UK GDPR), which establishes extensive operator due diligence obligations, data protection impact assessments, and applicable rigorous cross border transfer obligations.[16] The UK model more firmly establishes accountability and proactive measures to mitigate risk while setting clear obligations for multinational M&A transactions. This comparative analysis illustrates the considerations and hurdles for India, as it builds its emerging data privacy framework in context or consideration with a more established U.S. and U.K. systems.

[13] Anita Åkerman, Cultural Compatibility in Cross-Border M&A: Addressing the Gaps in Due Diligence for Successful Integration, (2025), https://urn.fi/URN:NBN:fi:amk-2025060219458
[14] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[15] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (West 2023).
[16] U.K. Gen. Data Prot. Regul., SI 2018/978 (UK).

ISSN: 2582-6433

STATEMENT OF PROBLEM:

In contemporary mergers and acquisitions, personal data increasingly functions as both a valuable commercial asset and a potential source of legal exposure. As companies rely more heavily on data-driven business models, compliance with data protection norms has become a central concern in M&A transactions. Despite this shift, Indian due diligence practices have continued to focus primarily on financial disclosures, regulatory approvals, and contractual obligations, often overlooking data privacy-related risks.

The introduction of the Digital Personal Data Protection Act, 2023 marks a substantial transformation in India's data protection regime by establishing new compliance standards and liability frameworks. However, the legislation does not clearly delineate the role of data privacy considerations within the due diligence process for M&A transactions, leaving acquiring entities uncertain about the extent of their obligations. This lack of clarity becomes particularly acute in cross-border transactions, where Indian acquirers must reconcile domestic requirements with multiple international data protection regimes. In the absence of specific statutory guidance, acquirers face heightened risks of post-acquisition liability and regulatory scrutiny. This study evaluates whether the existing Indian legal framework adequately addresses data privacy due diligence in M&A transactions and considers the extent to which international approaches may offer useful guidance.

RESEARCH QUESTION:

1. What are the data privacy–related due diligence obligations in M&A transactions under Indian law?
2. How does the DPDP Act, 2023 impact data disclosure and liability allocation in M&A due diligence?
3. How do EU (GDPR) and US approaches address data privacy risks in M&A transactions?
4. What reforms or best practices can strengthen data privacy due diligence in Indian M&A?

1. DATA PRIVACY AS AN M&A RISK:

Data privacy in mergers and acquisitions is one of the biggest risks nowadays as most of the times target companies hold and process large amounts of personal, sensitive, and commercially confidential data. The buying company doing its due diligence would need to

ISSN: 2582-6433

verify how well the target company has been complying with its data protection obligations, e.g. if it collects data lawfully, has valid consents, limits the purposes, follows retention rules, and manages cross border data transfers properly. A non-compliance situation present a risk for the purchaser in that the latter may become the subject of regulatory enforcement, get exposed to payment of sanctions, be liable for civil claims, and suffer reputational damage each of which may affect the fair value and the price of the acquisition significantly, if not be the reason for its collapse.[17]

The exposure to risk does not end at the time of closing since data assets as well as the related liabilities generally become the acquirer's concern. Hence, old compliance failures or insufficient cybersecurity may continue to place the company at risk even after the deal has been completed.[18] Therefore, privacy issues are becoming an important factor that shapes the deal through precisely negotiated representations and warranties, indemnity clauses, conditions precedent, and integration plans after the transaction. Recognizing data privacy as a major M&A risk leads to compliance with regulators, reduces the potential for claims arising from hidden risks, and recognizes data as a valuable asset that can be used responsibly and strategically in the combined entity.[19]

1.1 Concept and Regulatory Framework of Data Privacy Risk in M&A:

One of the main dangers of data privacy in mergers and acquisitions comes from the transfer, integration, and future use of personal information that was in the possession of the target company. In such deals, personal data is essentially a commercial asset of great value, although its use is subject to strict data protection laws.

Most commonly, the risks occur if the target has been collecting or processing data without getting proper consent, going beyond the purposes allowed, keeping the data for longer than what is lawful, or having inadequate security measures. Such breaches of compliance not only reduce the commercial value of the data but also create liabilities for the buyer, for instance, facing the authorities, contractual issues, and limitations on the post-merger use of the data.

Consequently, privacy compliance has now become a crucial point in legal due diligence that is impacting valuation, deal architecture, and post, acquisition integration strategies, directly.

[17] James A. Sherer, Taylor M. Hoffman & Eugenio E. Ortiz, Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, E-Discovery, and Information Governance into Due Diligence Practices, 21 Rich. J.L. & Tech. 5 (2015), https://jolt.richmond.edu

[18] Emil Hansson, Data Protection Considerations in the Pre-Merger Process: Due Diligence and Merger Assessment (M.A. Thesis, Lund Univ., 2024), https://lup.lub.lu.se

[19] Yuan Sun, Data Security and Mergers and Acquisitions (M.Phil. Thesis, Lingnan Univ., Aug. 23, 2021), https://commons.ln.edu.hk

ISSN: 2582-6433

The governance of data privacy risks in M&A is located at the intersection of domestic and foreign laws. On a global level, instruments like the EU General Data Protection Regulation (GDPR) set very high standards for legitimate processing, transparency, data minimisation, cross, border data transfers, and accountability, with heavy fines in case of violations.

India's Digital Personal Data Protection Act, 2023, places new duties on "data fiduciaries" in terms of getting lettings, data security, and reporting data breach thus even after corporate restructurings and business transfers, these obligations are there. Besides this, additional sector, specific rules and contractual data protection clauses raise the level of compliance even more. In short, these are forcing buyers to: carry out privacy risk assessment in a systematic manner, to embed privacy safeguards appropriately in the transaction documentation and to keep compliance going so as to reduce both regulatory and financial risk throughout the M&A lifecycle.

1.2 Data Privacy Risks During Due Diligence and Transaction Structuring:

During the due diligence phase of a merger or acquisition, data privacy issues are one of the most common concerns when the target company has to share personal data of its customers, employees, and third parties with the acquiring company. Any such information sharing must be in strict compliance with the relevant data protection laws and be limited to only the data necessary for the due diligence purpose as overly generous or unrestricted sharing could thus be considered a violation by the regulators.[20] Generally, the typical problems include no consent, purpose limitation or data retention requirements have been ignored, the company has a weak cybersecurity infrastructure, there have been data breaches that are either unreported or inadequately reported, and non, compliant cross, border data transfers. If these data privacy risks are not identified at the diligence stage, they may result in the improper valuation of the deal and the purchaser could be consequently exposed to regulatory enforcement actions or claims by the regulator or other private parties after the completion.[21]

In order to mitigate these worries, transaction frameworks are progressively incorporating agreements, level of data protection safeguards. Usually, the majority of the purchase agreements contain specific representations and warranties about compliance with data protection standards, as well as disclosure of any previous breaches and regulatory

[20] Regulation (EU) 2016/679, General Data Protection Regulation arts. 5, 6, 13–15, 32, 44–49, 2016 O.J. (L 119) 1, available at https://eur-lex.europa.eu

[21] European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679 (May 4, 2020), available at https://edpb.europa.eu

ISSN: 2582-6433

communications.[22] However, the parties tend to use indemnities, escrow arrangements, and conditions precedent to privacy and related risk allocations they have identified, while interim covenants may require the adoption of. At times, the amount and nature of the target's data and associated liabilities determine the choice between an asset acquisition and a share purchase. Therefore, by incorporating data protection issues into both due diligence and deal structuring, the parties are not only able to handle regulatory risks in an effective manner but also to continue processing data in a legitimate way post, transaction.[23]

1.3 Employee, Customer and Other Stakeholder Data Risks

People, data risks in M&A mainly arise from gathering, transferring and later processing of sensitive personal information such as employee identity details, financial information, health data and performance evaluation records. At the same time both in the due diligence and post merger integration phases the disclosure or use of such employee data might violate data protection, labour laws and other legal obligations if done without a proper legal basis and adequate technical and organisational measures being in place. These risks are further aggravated when employee data is shared within corporate groups, crosses jurisdictions, or is held for longer than the legally allowed period, thus increasing the chances of regulatory investigation, employee grievances, and loss of trust in the workforce.[24]

Customer and other stakeholder datasuch as vendors, users, and commercial partnersraise similar issues that are often heightened by the amount of data involved and the company's reliance on data, based operations. If there are shortcomings in agreement management, limiting the purpose for which the data is used, data security, or control over third party access, these may limit the acquirer's capacity to combine, repurpose or commercially exploit the data after the transaction. Besides that, already existing contractual obligations, privacy disclosures, and regulatory frameworks specific to the sector often limit the transfer or subsequent use of stakeholder data. Poor risk management in this area can, therefore, lead to regulatory enforcement, contractual liability, loss of reputation, and continued operational restrictions in the post, merger stage.[25]

[22] Digital Personal Data Protection Act, 2023, No. 22 of 2023, INDIA CODE (2023), available at https://www.indiacode.nic.in

[23] Organisation for Economic Co-operation and Development, OECD Privacy Guidelines (2013), available at https://www.oecd.org

[24] Digital Personal Data Protection Act, 2023, No. 22 of 2023, INDIA CODE (2023), available at https://www.indiacode.nic.in

[25] International Labour Organization, Protecting Workers' Personal Data: An ILO Code of Practice (1997), available at https://www.ilo.org

ISSN: 2582-6433

1.4 Post-Closing Integration, Governance and Reputational Risk

Post, closing integration can become a major source of data privacy risks especially when the acquirer begins the consolidation of information systems, databases, and operational processes across the two merged entities. The use of integrated datasets without, check if the data obtained previously was fit for the different purposes to which it is now used, or without obtaining new permissions if required, may be in violation of fundamental data protection principles. Different privacy policies, a lack of adequate cybersecurity measures, and a slow response to or identification of data breaches can still escalate the risk of regulatory sanctions as well as operational losses.[26] Therefore, dealing with these risks during the integration phase demands thorough data mapping, the harmonization of privacy policies, and the setting up of appropriate security and compliance measures to ensure legitimate and secure data processing. Firstly, it is important to note that continuously poorly handling data privacy after closing has broader governance and reputation risks that go beyond just regulatory compliance.[27]

Any data breach, regulatory penalty, or publicly disclosed violation of data privacy that comes to light will significantly damage the trust of the stakeholders and the reputation of the company. This will especially be the case if the business model is highly dependent on its access and use of data. Therefore, it is no surprise that boards and C, level executives are now being called upon to provide an active oversight of data governance by setting clear responsibilities and accountability, establishing internal audit functions, and ensuring regular compliance reporting. Integrating data privacy in the corporate governance framework is not only a tool for the risk control of the law side of the business. It is a great factor for the reputational recovery and the continuity of the company, in case of the merger and acquisition stage.[28]

2. Indian Legal Framework Governing Data Privacy in M&A

In India, the regulation of data privacy in mergers and acquisitions is part of a changing legal framework where personal data is on one side considered a valuable corporate asset and on the other side a potential source of legal exposure. M&A activities involve the transferring or ongoing processing of personal data such as that of employees, customers, and business

[26] James A. Sherer, Taylor M. Hoffman & Eugenio E. Ortiz, Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, E-Discovery, and Information Governance into Due Diligence Practices, 21 Rich. J.L. & Tech. 5 (2015), available at https://jolt.richmond.edu

[27] Emil Hansson, Data Protection Considerations in the Pre-Merger Process: Due Diligence and Merger Assessment (M.A. Thesis, Lund Univ., 2024), available at https://lup.lub.lu.se

[28] Regulation (EU) 2016/679, General Data Protection Regulation arts. 5, 6, 24, 25, 32–34, 2016 O.J. (L 119) 1, available at https://eur-lex.europa.eu

ISSN: 2582-6433

associates, thus making data protection compliance a major concern of the transaction. The present, era Digital Personal Data Protection Act, 2023 A.K.A. DPDP Act had strengthened the data protection regime in India by providing for the lawful processing of data, consent management, data security, and accountability of organizations, which in the context of corporate restructuring and business transfers, is quite relevant. Apart from that, sector, specific regulatory rules, contractual data protection obligations, and the more general corporate governance principles control the extent to which data can be disclosed, transferred, and integrated during M&A transactions, hence data privacy is one of the main legal risks which run from the due diligence phase to the post, closing integration.

2.1 Statutory Framework: DPDP Act, 2023 in the M&A Context

The Digital Personal Data Protection Act, 2023 (DPDP Act) is the main piece of legislation that establishes the statutory data protection regime in India and is directly relevant to mergers and acquisitions. By controlling the use of digital personal data, the Act is applicable to 'data fiduciaries', the term encompasses companies which are, among other things, involved in mergers, acquisitions, amalgamations, and business transfers. For M&A transactions, employee, customer and other stakeholder personal data of the target that is held by the target remains covered under the DPDP Act, and even a change of ownership or control does not relieve the parties of the obligation to handle such data in a lawful, fair, and purpose, bound manner.[29] Basic principles like purpose limitation, data minimization, storage limitation, and the necessity for reasonable security safeguards limit the transfer, reuse, or combination of personal data after a transaction. Ignoring these requirements not only results in hefty fines but also the issuance of regulators' orders that will have an immediate impact on transaction valuation and risk allocation.[30]

The Act further furthers the strengthening of governance and accountability standards which, among other things, change the ways through which the transactions are carried out and the businesses combined after the closing. The requirements for data breach notification, the appointment of data protection officers for major data fiduciaries, and the provision of easily accessible grievance redressal mechanisms are expected to be continued from the post, acquisition stage.[31] Transaction documentation thus, gradually, details not just DPDP, specific

[29] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, §§ 2(i), 6, 8, 9 (India), https://www.meity.gov.in/data-protection-framework

[30] Ministry of Electronics & Information Technology, Digital Personal Data Protection Act, 2023 – Overview and Key Provisions, Government of India, https://www.meity.gov.in/digital-personal-data-protection-act-2023

[31] Digital Personal Data Protection Act, 2023, §§ 8(5), 10, 11 (India) (imposing obligations relating to security safeguards, breach notification, and grievance redressal), https://egazette.nic.in

ISSN: 2582-6433

representations, warranties, and indemnities, but also post, closing agreements, committed to corrective action implementation. Hence, the DPDP Act positions data protection as a premier statutory issue, thereby, forcing buyers to integrate privacy compliance not only in pre, transaction due diligence but also in post, merger governance frameworks.[32]

2.2 Consent, Purpose Limitation and Allocation of Liability on Business Transfer

If we consider merger and acquisition which primarily deals with business entity as a whole, the extent and validity of the consent which determines the processing of personal data is the real issue. Hence the Digital Personal Data Protection Act, 2023, an individual personal data can be processed only with their consent. During a merger or acquisition deal where the business is transferred, if the consent is very limited or if it is expressly only giving the right to the transferor, the acquirer may have to inform about privacy changes or obtain new consent, especially if the use of data after the acquisition deviates from the original purposes.[33]

Purpose limitation puts a further limit on the use of the transferred data. The personal data that has been initially collected with a liaison of objective cannot be repurposed by the acquirer in a manner that is incompatible without meeting the conditions stipulated in the statute. Most of the time, this prevents the merging of different data sets, the use of customer information for commercial purposes, and the running of data, driven business models unless a compliance check is done. Ignoring the purpose limitation not only makes the regulatory authorities point a finger at you but your acts may also destroy the commercial value of the data obtained.[34]

It is very important that the responsibility for data protection be clearly assigned when one is structuring a transaction, especially if one has to operate within these restrictions. In most cases, the buyers want to protect themselves by way of representations, warranties, and indemnities that will cover consent failures, data protection breaches, and regulatory sanctions, as the defects of the pre, closing period which is non, compliant may only be, discovered post closing.[35] Besides, the parties may also agree to use escrow arrangements or price adjustments

[32] Shardul Amarchand Mangaldas & Co., India: Data Protection Considerations in M&A Transactions Under the DPDP Act, 2023, Mondaq (2023), https://www.mondaq.com/india/data-protection/1360000

[33] Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018) (India) (emphasizing consent specificity and limits on downstream use of personal data in commercial transactions), https://www.meity.gov.in/content/committee-reports

[34] Deloitte India, India's Digital Personal Data Protection Act, 2023: Key Implications for M&A and Business Transfers (2023) (analyzing consent continuity, change-in-purpose risks, and post-closing compliance exposure), https://www2.deloitte.com/in/en/pages/legal/articles/dpdp-act-2023.html

[35] Internet Freedom Foundation, Understanding Consent and Purpose Limitation Under India's DPDP Act (2023) (critiquing reuse of personal data following structural corporate changes), https://internetfreedom.in.

ISSN: 2582-6433

as a means of dealing with residual exposure.[36] A well, thought, through splitting of the data, related, liability not only helps to ensure the, regulatory, compliance, but at, the same, time acts as a, risk, sharing, instrument between the, grantor, and the, grantee, in the, business, transfer, transactions.

2.3 Corporate Law Overlay: Companies Act, 2013 and Contractual Warranties/Indemnities

The Companies Act, 2013 gives a big corporate law aspect to the issue of data privacy compliance in mergers and acquisitions by setting the rules that govern the approval processes, disclosure requirements, and fiduciary responsibilities in mergers, amalgamations, and business transfers. Directors are required to act honestly and with due care when they are looking after the interests of the company and its stakeholders, an obligation that nowadays also covers the protection of data assets and the handling of privacy risks.[37] In the schemes which are approved by the courts or tribunals under the Act, like mergers and demergers, the handing over of data has to meet the statutory conditions and cannot be used as an excuse for not fulfilling data protection legislation. If at this point they ignore data privacy considerations, that is going to be a mistake in governance and both the company and its directors can be held legally responsible.[38]

Against that background, the role of contractual risk, allocation mechanisms is considerably heightened. Very often, transaction agreements have a number of representations and warranties regarding the parties' adherence to the data protection laws, no undisclosed data breach, a properly functioning consent framework, and the sufficiency of cybersecurity controls. If the investigation uncovers a situation that entails an enhanced level of risk, the parties, as a rule, enter into indemnities, escrow deposits or a combination of these together with covenants to a specific part, so that the acquirer is effectively protected from the regulatory, third, party, and remediation costs issues related to pre, closing non, compliance. Both the statutory regime under the Companies Act and the well, considered contractual safeguards point to data privacy not simply as a matter of regulatory compliance, but as a main

[36] PwC India, Data Protection in India: Transactional Risk Allocation Under the DPDP Act (2023) (discussing indemnities, escrow mechanisms, and valuation impact of data protection non-compliance), https://www.pwc.in/industries/technology/publications.html

[37] Supreme Court of India, Miheer H. Mafatlal v. Mafatlal Industries Ltd., (1997) 1 S.C.C. 579 (India) (holding that court/tribunal approval of schemes does not dispense with compliance with other applicable laws), https://indiankanoon.org

[38] Khaitan & Co., Representations, Warranties and Indemnities in Indian M&A Transactions: Emerging Focus on Data and Cyber Risks (2023), https://www.khaitanco.com/thought-leaderships

ISSN: 2582-6433

issue of corporate governance and M&A risk allocation.[39]

2.4 Regulatory Uncertainty, Enforcement Gaps and Residual Risk in M&A Deals

Regulatory uncertainty remains a major obstacle to mergers and acquisitions despite the fact that data protection standards have been steadily improved. It especially holds for countries like India where the privacy regime is undergoing a change. Several points of the Digital Personal Data Protection Act, 2023, such as the use of personal data in corporate restructuring, the criteria for being classified as a significant data fiduciary, and the definitions of legitimate uses allowed, will still have to be decided through subordinate legislation and regulatory interpretation. This vagueness complicates the due diligence exercise and restricts the acquirer's capability to properly assess and price the privacy, thereby, related risk at the deal, structuring stage.[40]

Uncertainty is being made worse by the different enforcement practices. Not having a clear legal basis for a regulation against M&A, the related data transfers, and the delay in the institutional set, up of the Data Protection Board all lead to the enforcement goals and penalty assessments being largely uncharted territory. Hence, this scenario may restrict the range of a regulatory intervention now, but it will, actually, raise the risk later when a deeper look at data practices may be initiated by a violation, a complaint, or a change in the enforcement mood.

Therefore, regardless of how thorough your due diligence is and contract negotiations are, there will always be some leftover risk of data privacy.[41] Through representations, warranties, and indemnities, you may only be able to protect yourself from the risk of regulatory fines, loss of reputation, or business restrictions drifting back to a very small extent. The proper management of data privacy risk in merger and acquisition should not only be a matter of compliance with the law but should also involve strategic risk assessment and post, transaction control.[42]

[39] Nishith Desai Associates, Director Liability and Governance Risks in Indian M&A Transactions (2022) (examining breach of duty, disclosure failures, and risk allocation through contractual protections), https://www.nishithdesai.com/knowledge-centre.

[40] Standing Committee on Communications and Information Technology, Review of the Digital Personal Data Protection Bill, 2023, Lok Sabha Secretariat (2023) (highlighting reliance on future rule-making and delegated legislation for operational clarity), https://loksabhadocs.nic.in

[41] Vidhi Centre for Legal Policy, India's DPDP Act: Open Questions on Enforcement, Classification of Data Fiduciaries and Regulatory Design (2023) (analyzing ambiguity around "significant data fiduciary" designation and legitimate uses), https://vidhilegalpolicy.in

[42] EY India, Managing Residual Data Privacy Risk in M&A Transactions Amid Regulatory Uncertainty (2024) (examining limits of contractual protections and the need for post-closing governance frameworks), https://www.ey.com/en_in

ISSN: 2582-6433

3 Due Diligence Obligations in Indian M&A Practice

Due diligence is the main instrument in Indian M & A (Mergers and Acquisitions) for figuring out the legal, regulatory, and operational risks that pertain to the target entity. Besides checking the corporate documentation and financial disclosures, purchasers have been looking more and more at whether the target has complied with data protection requirements, sector, specific regulatory norms, and existing contractual commitments. This investigation usually implies that the acquirer goes through privacy policies, consent mechanisms, data processing practices, cybersecurity controls, records of past data breaches, and any ongoing or prior regulatory inquiries. The acquirer can thus determine whether the target's operations are in line with the statutory obligations as well as the accepted industry standards.[43]

The discovery of due diligence findings and the revelations therein significantly impact how the deal is structured and how the risks are shared among the parties involved. Moreover, in situations involving personal data issues, integration plans following the merger will also be influenced by the alterations in due diligence since the latter highlights the areas where a remedy is most urgently required.[44] Hence, due diligence in Indian M&A deals is far more than just verifying the accuracy of the statements; it is also a strategic instrument for managing post, transaction legal risks and ensuring continuous regulatory compliance after the completion of the deal.

3.1 Scope of Data Privacy in Due Diligence

Data privacy due diligence is important for Indian M&A transactions. One aspect of it is to look very deeply at how the target company manages data, and this is done to find out if there are any risks from the point of view of regulations, laws, and operations. Among other things, this would mean going through the policies and procedures of the company that provide the framework for also, the first few paragraphs, the company is likely to focus on employees, customers, and other individuals whose personal data are being processed. The main points of scrutiny will be the forward to the Digital Personal Data Protection Act, 2023, and, at the same

[43] Medianama, Explained: Why Enforcement Under India's New Data Protection Law Will Take Time (2023) (discussing the delayed operationalization of the Data Protection Board and its implications for enforcement certainty), https://www.medianama.com

[44] EY India, Managing Residual Data Privacy Risk in M&A Transactions Amid Regulatory Uncertainty (2024) (examining limits of contractual protections and the need for post-closing governance frameworks), https://www.ey.com/en_in

ISSN: 2582-6433

time, other compliances that are requisite for the industry in which the company operates.[45] Cybersecurity is a significant aspect of due diligence. Besides that, it also means examining the records of previous data breaches, evaluating the incident response protocols, and checking for any regulatory notices or investigations. Extensive review is taking place of the agreements with third, party vendors, data processing contracts, and other contractual obligations relating to data protection to ensure that the target's procedures do not impose any uncovered liabilities on the acquirer. After comprehensively scrutinizing these matters, purchasers can identify non, compliance issues, evaluate the level of risks, and insert into the transaction the correct representations, warranties, indemnities, and post, closing remediation obligations, thereby not only complying with the law but also protecting the commercial value of the acquired data assets.[46]

3.2 Data Mapping, Breach History, Consent Audits

Strong data mapping is at the heart of Indian M&A practitioners' data privacy diligence when they combine forces. Simply put, personal data mapping is a data flow exercise that tracks data held by a target from start to finish, i.e. from data location at the source, data type, storage environment, processing activities, transfers (especially third, party), and current retention practices. A purchaser can, therefore, identify mistakes to compliance, evaluate the risk from the regulators and plan a less disruptive post, merger integration, thus satisfying processing activity compliance under the DPDP Act, 2023 through this mapping.

Breach history assessment thoroughly examines instances of data leaks, unauthorized access, or cybersecurity being compromised, and the target's response, e.g. informing regulators and those affected. Reviewing the breach history of a company enables the acquirer to estimate potential regulatory penalties, lawsuit risks, and the resultant harm to the brand of the combined entity after completion of the transaction.[47]

Consent audits mainly concentrate on checking if the target has obtained proper, specific, and informed consent for the initial collection and subsequent use of personal data, especially personal data that will be used or transferred after the acquisition. Besides, the audits check

[45] AZB & Partners, Data Privacy and Cybersecurity Due Diligence in Indian M&A Transactions (2023) (detailing review of breach history, vendor contracts, and regulatory exposure during acquisitions), https://www.azbpartners.com/insights

[46] KPMG India, Data Privacy and Cyber Risk: Key Due Diligence Considerations for M&A (2023) (discussing valuation impact and post-closing remediation linked to data non-compliance), https://kpmg.com/in.

[47] NASSCOM, Data Protection and Privacy in India: Due Diligence and Risk Assessment Framework (2023) (recommending breach history reviews and consent audits as part of M&A diligence), https://www.nasscom.in/knowledge-center/publications

ISSN: 2582-6433

whether the existing consents are sufficient for the intended new purposes or cross, border transfers, and they point out the consents where consent has to be re, obtained or privacy notices have to be updated.[48] Basically, these investigative elements together make up the main parts of data privacy due diligence. That way buyers are enabled to evaluate the risk, negotiate appropriate safeguards, and stay compliant with the regulations during the whole transaction process.

3.3 Contractual Tools: Representations, Warranties, Indemnities:

Contractual safeguards are the main tools for dividing and controlling data privacy risk in M&A transactions. Through representations, the target has to legally confirm that its data protection compliance is truthful, including conformity with the Digital Personal Data Protection Act, 2023, the strength of the consent mechanisms, the adequacy of the cybersecurity measures, and the non, existence of any data, related incidents that are still to be resolved. These kinds of assurances enable a purchaser to consider the targets legal and operational risks.[49]

Warranties are statements of fact that the data privacy, related information is accurate at the time of signing or closing; if later on such information is found to be incorrect, e.g., due to non, disclosure of non, compliance or the disclosure of former breaches, the buyer may be able to resort to contractual remedies. Indemnities in that case should be seen as the transferring of the financial burden in respect of certain pre, closing liabilities, e.g., regulatory fines, third, party claims, or costs of litigation resulting from historical privacy failures. In a nutshell, representations, warranties, and indemnities spell out the commitments, divide the residual risk, and provide the purchaser with compensation mechanisms that basically protect the purchaser from the hidden legal, financial, and reputational damages existing at the time of the transaction.[50]

3.4 Role of Data Protection Officers

Data Protection Officers (DPOs) play a vital role in identifying and managing the risks associated with breaches of data privacy during M&A transactions not only at the point of due

[48] Trilegal, Consent Management and Data Transfers in Indian M&A Transactions (2023) (analyzing validity of legacy consents, change-of-purpose risks, and post-acquisition compliance steps), https://trilegal.com/knowledge-centre

[49] Clifford Chance, Allocating Data Protection Risk Through Representations, Warranties and Indemnities in M&A Transactions (2023) (discussing disclosure of breaches, compliance warranties, and indemnity structuring for privacy liabilities), https://www.cliffordchance.com/insights.html

[50] Allen & Overy, Data Privacy as a Deal Risk: Contractual Protection in Corporate Acquisitions (2022) (examining how privacy representations and indemnities operate as financial risk-shifting tools), https://www.allenovery.com/en-gb/global/news-and-insights.

ISSN: 2582-6433

diligence but also throughout the changeover period. As per the DPDP Act,2023 a DPO is a major where data fiduciary is entitled with the duty to process data operations and develop and implement framework for privacy policy.[51] During a takeover, the DPO sometimes acts as the intermediary between the buyer and the seller, and through the DPO, the party gets a very detailed exposure to data flows, consent mechanisms, breach record, and security measures which, in turn, allow the party to gauge the extent of privacy risk.

They do a thorough job with a broad scope. Post closing, DPOs are the ones who initiate the embedding of privacy practices between the target and the acquirer. Moreover, they ensure that data transfers are based on a legitimate ground, privacy notices, if changed, are updated and consent management systems are kept very efficient. They have a role in regulatory reporting and breach notification compliance as per the requirements of the applicable laws that they align with.[52] However, DPOs have a crucial role in regulatory reporting and breach notification compliance as per the requirements of the applicable laws that they align with. In short, a person who can communicate effectively between business operations, compliance with the laws, and engagement with the regulatory can through the role of DPO help to mitigate the risk of enforcement action, improve governance and even contribute to the maintenance of stakeholder trust throughout the M&A process.[53]

4 Comparative Analysis: EU And US Approaches

General Data Protection Regulation (GDPR) is the main data privacy legislation in mergers and acquisitions (M&A) within the European Union. Since the GDPR stresses the importance of lawful grounds, accurate purpose, data minimization, and very strict consent requirements, the acquiring parties thus need to deeply rejustify the sharing of data, identify cross, border transfer safeguards, and keep very detailed compliance records, these and more will directly influence the deal structuring, contractual protection, and integration planning.[54]

[51] European Data Protection Board, Guidelines on Data Protection Officers (DPOs) (2017) (clarifying the intermediary and oversight role of DPOs during organizational changes and corporate restructuring), https://edpb.europa.eu

[52] McKinsey & Company, Why Data Governance and DPO Functions Matter in M&A Integrations (2022) (highlighting how DPO-led governance reduces regulatory and reputational risk in transactions), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights

[53] International Association of Privacy Professionals, The DPO's Role in Mergers, Acquisitions and Corporate Restructuring (2021) (discussing due diligence support, data flow analysis, and post-merger integration responsibilities), https://iapp.org/resources/article/dpo-ma

[54] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), arts. 5–6, 44–49, 2016 O.J. (L 119) 1 (EU) (laying down lawful bases, purpose limitation, and cross-border transfer safeguards relevant to M&A data sharing), https://eur-lex.europa.eu

ISSN: 2582-6433

Instead, the U.S. has a system of federal, state, and specific sector regulations that govern the same areas as a more unified law internationally. The California Consumer Privacy Act (CCPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm, Leach, Bliley Act (GLBA) are examples of acts that only focus on specific types of data or industries, thus M&A due diligence is mainly concerned with identifying which laws are applicable, verifying that the contracts are compliant with them, and assessing the likelihood of the case being enforced or litigated.[55] Nevertheless, there are a lot of U.S. laws which favor disclosure and opt, out mechanisms over consent in the same manner as the GDPR. Consequently, the parties are usually given more freedom in a structural sense but, at the same time, they also have to deal with more interpretative and jurisdictional problems, especially, when it comes to cross, border or multi, state transactions.

4.1 European Union (GDPR):

Under the European Union General Data Protection Regulation (GDPR), data protection is more of a central compliance requirement in M&A deals than just a contractual risk allocation. The handing over of personal data during due diligence as well as post, integration is processing, thus it needs to be based on a valid legal ground such as legitimate interests, necessity of the contract, or consent. Buyers are required to observe the restrictions on the purpose of the data, the amount of data, and openness when digging into staff or client data pre, closing, and any later mixing or reusing of that data must still be compatible with the original purposes or be supported by a new legal basis.[56]

There is no doubt GDPR's accountability and governance framework play a major role in how parties approach the structuring of deals. For instance, the parties involved must keep proper records of processing activities, carry out data protection impact assessments (DPIAs) when there is high, risk processing, and adhere to breach notification timelines that are very strict in relation to supervisory authorities and data subjects. Furthermore, cross, border M&A operations involving personal data of the EU must comply with rules on international transfers and use such tools as adequacy decisions, standard contractual clauses, or binding corporate

[55] Federal Trade Commission, Privacy and Data Security Update: Implications for Business Transactions (2021) (discussing sector-specific privacy enforcement and litigation risk in U.S. corporate acquisitions), https://www.ftc.gov/business-guidance/privacy-security.

[56] European Data Protection Board, Guidelines 8/2020 on the Targeting of Social Media Users (2020) (clarifying assessment of legitimate interests and necessity tests relevant for pre-closing due diligence access to personal data), https://edpb.europa.eu

ISSN: 2582-6433

rules.[57] Due to the extraterritorial nature of GDPR and the possibility of very large administrative fines, compliance with EU data protection laws is often a deciding factor in the valuation, the setting of representations and warranties, and the way post, merger integration plans are laid out.[58]

4.2 US (CCPA)

The United States has a decentralized, sector, specific approach to managing data privacy in mergers and acquisitions instead of having one single comprehensive law. To be affected by these situations is a mix of different federal and state laws, for example, the California Consumer Privacy Act (CCPA) and its amendments for consumer data, HIPAA for health information, and the Gramm, Leach, Bliley Act (GLBA) for financial data.[59] Thus, the bulk of M&A due diligence is concerned with identifying which state or sectoral rules are applicable to the target's business, verifying compliance with notice and disclosure requirements, and examining data, related contracts for use and sharing clauses.

A defining characteristic of the US model is its emphasis on disclosure, fairness, and consumer protection, rather than on a uniform consent driven standard. Practitioners practically and regularly measure privacy risk through two questions: (1) the extent to which the targets privacy policies truthfully and fully reflect its data practices; and (2) whether planned reuse of collected data after a takeover corresponds with those statements.[60] As the main enforcer, The Federal Trade Commission (FTC) intervenes frequently when a company uses deceptive or unfair methods to consumers and thus, among other things, when data usage is materially changed following an acquisition without individuals being properly informed or given the option to consent.

Consequently, US M&A deals greatly rely on the representations, warranties, and post closing disclosure to reallocate and control the privacy risk, thus generating a structure that is

[57] European Commission, International Transfers of Personal Data Under the GDPR (2023) (explaining adequacy decisions, standard contractual clauses, and binding corporate rules for cross-border corporate restructuring), https://commission.europa.eu/law/law-topic/data-protection_en.

[58] Regulation (EU) 2016/679, arts. 30, 35, 33–34 (EU) (mandating records of processing activities, data protection impact assessments, and strict breach notification timelines), https://eur-lex.europa.eu

[59] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199.100 (West 2024) (establishing notice, disclosure, and opt-out–based consumer rights relevant to M&A data transfers), https://oag.ca.gov/privacy/ccpa

[60] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 15 U.S.C.) (imposing privacy and safeguarding obligations on financial institutions in corporate transactions), https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act

ISSN: 2582-6433

technically very adaptable but at the same time very much influenced by enforcement.[61]

5 Challenges in Cross-Border M&A Transactions

When an acquisition crosses borders, the resulting merger and acquisition (M&A) activities raise complex issues of data privacy because different, and at times contradictory, legal systems are applied simultaneously. The acquiring companies have to face different standards of obtaining consent, legitimate bases for processing, requirements for data localisation, and rules for cross, border transfers under such instruments as the EU GDPR, Indias DPDP Act, 2023, and various US sectoral laws. It may even be difficult to lawfully share data during the due diligence phase because pre, closing access to personal data might have to be kept limited, anonymous, or done by means of secure data rooms, and it should be backed up by legitimate interest assessments. Such differences raise the costs of compliance and therefore, have the potential to greatly influence the timetable and structuring decisions of a deal.[62]

Post closing integration usually makes these problems worse, because the integration of global IT systems and databases could be the grounds for international data transfer restrictions and thus require several additional safeguards, e.g., standard contractual clauses or binding corporate rules.The persistent unclear nature of the rules, unfair enforcement practices, and the strong territorial reach of some laws increase the risk of overlapping liabilities and thus getting the authorities to look more closely. Consequently, cross border M&A needs the legal, technical, and governance measures to be so well coordinated that privacy compliance is ensured across different jurisdictions without compromising the commercial value of data assets and the continuity of the business.[63]

5.1 Data Localisation

Data localisation refers to the laws that indicate if certain types of data need to be stored, processed, or kept within a certain country's borders. In relation to M&A, such regulations might heavily influence the structuring of a deal and the post, merger integration phases, particularly if the target company is a multi, country player. Localisation requirements may

[61] Federal Trade Commission, Protecting Consumer Privacy in Corporate Transactions (2022) (explaining enforcement against deceptive or unfair changes in data use following mergers or acquisitions), https://www.ftc.gov/business-guidance/privacy-security.

[62] European Data Protection Supervisor, Guidelines on Data Transfers in Mergers and Acquisitions (2021) (recommending anonymization, data minimization, and secure data rooms during cross-border due diligence), https://edps.europa.eu

[63] Baker McKenzie, Cross-Border M&A and Data Privacy: Managing Multi-Jurisdictional Risk (2023) (analyzing conflicting legal standards, enforcement overlap, and post-merger integration challenges), https://www.bakermckenzie.com/en/insight/publications.

ISSN: 2582-6433

refer to the transfer of personal or sensitive data across borders, thus limiting the possibility of data centralisation and raising the compliance costs of acquirers who are combining global IT infrastructures. Moreover, non, compliance with these regulations may result in regulatory sanctioning as well as the occurrence of practical problems in business operations; therefore, localisation risks should be thoroughly considered during due diligence and be reflected in the transaction planning stages of cross, border deals.[64]

5.2 Regulatory Conflict

Regulatory conflict in M&A arises basically when data protection and related regulatory regimes in different jurisdictions impose on the parties overlapping, divergent, or even contradictory obligations. An acquirer in a cross, border transaction could be in a position where one legal system allows or even encourages data sharing and centralisation, while another legal system demands very strict compliance with consent standards, local data storage requirements, or very limited data transfer controls.[65]

For example, one can imagine a situation where the use of the GDPR cross, border transfer mechanisms is in conflict with the local data storage requirements or the sector, specific rules in the target's country of origin. Such conflicts create doubt at the due diligence and post, closing integration stages, significantly increase the risk of inadvertent non, compliance, and very often result in the parties going for the most conservative structuring options, multiple contractual safeguards, and compliance measures which are highly customised and specific to each jurisdiction involved.[66]

5.3 Transfer of Liabilities

Data privacy liabilities remain a key part of the business and hence liabilities of the acquirer in most M&A transactions, particularly, in the cases of share deals and statutory mergers. Market regulators or third parties may still initiate actions for breaches, unresolved incidents, or improper consent frameworks post, closing even if the original misconduct that led to data protection violations occurred before the acquisition. If due diligence overlooks these problems

[64] Telecom Regulatory Authority of India, Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector (2018) (advocating localisation of sensitive telecom subscriber data with implications for foreign acquisitions), https://www.trai.gov.in

[65] Court of Justice of the European Union, Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II), Case C-311/18, ECLI:EU:C:2020:559 (2020) (invalidating the EU-US Privacy Shield and intensifying regulatory conflict in cross-border data transfers), https://curia.europa.eu

[66] Herbert Smith Freehills, Managing Conflicting Data Protection Obligations in Cross-Border M&A Transactions (2023) (analyzing conservative deal structuring and jurisdiction-specific safeguards adopted in response to regulatory conflict), https://www.herbertsmithfreehills.com

ISSN: 2582-6433

or transaction agreements are not satisfactorily adjusted to them, the risk is even greater. Therefore, buyers should clearly determine the level of privacy commitments they are taking over and demand from the seller, representations, warranties, and indemnities, which are particularly meant to cover non, compliance risks in the seller's history.[67]

5.4 Enforcement Risks

Enforcement risk in M&A arises from the prospect of post-acquisition scrutiny, sanctions, or remedial directions by data protection regulators. Authorities may open investigations in response to data breaches, consumer complaints, or material changes in data use following the transaction, especially in jurisdictions with assertive enforcement cultures such as the EU. In India, the evolving enforcement practice under the DPDP Act, 2023 creates additional uncertainty for acquirers about how and when regulators will intervene. These concerns are amplified in cross-border deals, where several regulators may claim jurisdiction, raising the prospect of parallel proceedings and significant reputational fallout for the combined entity.[68]

6. Recommendations and Best Practices

6.1 Mandatory Data Privacy Audits in M&A

Making data privacy audits a mandatory component of M&A due diligence would significantly reduce regulatory and transactional risk. Such audits should go beyond surface-level policy reviews and include detailed assessments of data mapping, consent validity, breach history, cybersecurity controls, third-party data sharing arrangements, and cross-border transfers. A structured audit allows acquirers to quantify privacy-related liabilities, assess the true commercial value of data assets, and identify compliance gaps that require remediation before or immediately after closing. Embedding privacy audits as a standard practice aligns M&A transactions with modern regulatory expectations and promotes informed decision-making in deal valuation and structuring.[69]

[67] Competition Commission of India, Combination Regulations: Guidance on Successor Liability and Post-Combination Compliance (2022) (illustrating how regulatory scrutiny may continue post-closing notwithstanding change in ownership), https://www.cci.gov.in

[68] World Bank, Enforcement of Data Protection Laws: Emerging Trends and Risks for Cross-Border Transactions (2021) (highlighting risks of parallel investigations, reputational harm, and regulatory uncertainty in multinational acquisitions), https://www.worldbank.org.

[69] International Association of Privacy Professionals, Privacy Audits and Assessments: A Risk-Based Approach for Corporate Transactions (2022) (advocating comprehensive privacy audits covering data mapping, consent, breaches, and third-party sharing in M&A), https://iapp.org/resources/article/privacy-audits-assessments

ISSN: 2582-6433

6.2 Regulatory Guidelines by Indian Authorities

Clear and sector-specific regulatory guidance from Indian authorities would help address uncertainty surrounding data transfers during mergers, amalgamations, and business transfers. Guidelines issued by the Data Protection Board of India or relevant ministries could clarify permissible data sharing during due diligence, treatment of consent upon change of control, and obligations of transferees post-acquisition. Such guidance would enhance predictability, reduce compliance ambiguity, and enable companies to structure transactions in a manner consistent with both corporate law and data protection obligations. Regulatory clarity would also encourage proactive compliance rather than reactive risk management.[70]

6.3 Standardised Due Diligence Checklists

Adopting standardised data privacy due diligence checklists can ensure consistency and thoroughness across M&A transactions. These checklists should cover statutory compliance under the DPDP Act, sectoral regulations, internal governance frameworks, data localisation requirements, breach management protocols, and contractual obligations with vendors and partners.[71] Standardisation helps reduce oversight, facilitates comparison across targets, and supports better risk allocation through transaction documents. For practitioners, such checklists serve as practical tools to integrate data privacy seamlessly into traditional legal and financial due diligence processes.

6.4 Safe Harbour Provisions

Introducing safe harbour provisions for M&A transactions would provide meaningful protection to acquirers who undertake good-faith compliance efforts. Safe harbours could limit regulatory penalties where the acquirer conducts reasonable data privacy due diligence, discloses identified risks to regulators when required, and commits to post-closing remediation within prescribed timelines. This approach recognises the practical challenges of uncovering legacy non-compliance and balances regulatory enforcement with commercial reality.[72] Safe harbour frameworks would incentivise proactive audits, transparency, and timely corrective

[70] Law Commission of India, Regulatory Reform and Delegated Legislation in Emerging Technology Laws (2023) (emphasizing the role of clear executive and sector-specific guidelines in reducing compliance uncertainty under new statutory regimes), https://lawcommissionofindia.nic.in

[71] Asian Development Bank, Good Regulatory Practices for Data Protection Compliance in Corporate Transactions (2021) (recommending standardized compliance checklists to improve consistency, transparency, and risk allocation in cross-border investments), https://www.adb.org

[72] Organisation for Economic Co-operation and Development, Safe Harbours and Regulatory Flexibility in Data Protection Enforcement (2020) (supporting conditional safe harbour mechanisms to encourage good-faith compliance and post-transaction remediation), https://www.oecd.org/digital/privacy

ISSN: 2582-6433

action, while reducing deterrence to investment and facilitating smoother business transfers. By offering conditional regulatory protection, safe harbour provisions could play a crucial role in strengthening India's M&A ecosystem while maintaining robust data protection standards.

7. Conclusion

This study has examined data privacy as an increasingly decisive factor in mergers and acquisitions, particularly within the Indian legal and regulatory context. The analysis demonstrates that data privacy due diligence under Indian law extends beyond conventional corporate and financial review to include a detailed assessment of how personal data is collected, processed, transferred, and secured by the target entity. Acquirers are required to evaluate compliance not only with statutory obligations under the Digital Personal Data Protection Act, 2023, but also with sector-specific regulations, contractual commitments, and broader principles of corporate governance.[73] Data privacy due diligence therefore operates as a critical risk-identification mechanism, shaping both transaction structuring and post-closing integration.

The enactment of the DPDP Act, 2023 has significantly altered the due diligence landscape by reinforcing consent requirements, purpose limitation, data minimisation, and accountability obligations that persist notwithstanding changes in corporate ownership. The Act clarifies that a transfer of control does not dilute data protection responsibilities, thereby increasing the likelihood that acquirers may inherit liabilities arising from historical non-compliance.[74] As a result, data disclosure during due diligence and the allocation of liability through representations, warranties, indemnities, and post-closing covenants have assumed greater prominence in M&A documentation. The DPDP framework thus positions data privacy as both a regulatory compliance issue and a transactional risk that directly influences valuation and deal certainty.[75]

A comparative assessment of the European Union and the United States further illustrates how

[73] Ministry of Electronics & Information Technology, Explanatory Statement on the Digital Personal Data Protection Act, 2023 (India) (emphasising continuity of data protection obligations notwithstanding change in control and the shift toward accountability-based compliance), https://www.meity.gov.in

[74] World Economic Forum, Global Data Governance and the Future of Corporate Transactions (2022) (recognising data as a strategic business asset and highlighting privacy due diligence as a determinant of deal value and sustainability), https://www.weforum.org

[75] European Commission, GDPR at Five: State of Enforcement and Compliance Culture in the EU (2023) (illustrating how mature enforcement practices influence transaction structuring and post-merger governance), https://commission.europa.eu

ISSN: 2582-6433

mature privacy regimes approach data privacy risks in M&A transactions. The GDPR's emphasis on accountability, transparency, and regulatory enforcement has led to well-established diligence practices and clearer expectations around liability transfer. In contrast, the United States' sectoral and enforcement-driven approach places greater reliance on disclosure obligations and post-transaction regulatory scrutiny. These comparative insights highlight the relative underdevelopment of Indian enforcement practice and underscore the need for clearer regulatory guidance tailored to corporate restructuring and business transfers. Despite the strengthening of India's statutory framework, regulatory uncertainty and limited enforcement precedent continue to create residual risk in M&A transactions. The absence of detailed rules on data treatment during corporate restructuring, evolving thresholds for significant data fiduciaries, and reliance on delegated legislation complicate due diligence assessments and risk pricing. This study therefore underscores the need for targeted reforms, including regulatory guidance on data transfers in M&A, standardised privacy due diligence checklists, and greater clarity on liability attribution in business transfers. Best practices such as mandatory data privacy audits, enhanced board-level oversight, and post-closing compliance reviews can further mitigate exposure and improve transactional certainty.[76]

Looking ahead, the growing reliance on data as a core business asset suggests that data-driven M&A transactions will continue to intensify both legal scrutiny and commercial risk. Effective management of data privacy in this context will require acquirers to move beyond formal compliance and adopt a governance-oriented approach that integrates privacy considerations across the transaction lifecycle.[77] Strengthening India's regulatory clarity and institutional enforcement capacity will be essential to ensuring that data-driven M&A activity remains both legally sustainable and economically efficient in the evolving digital economy.

[76] Vidhi Centre for Legal Policy, Implementing India's Data Protection Law: Institutional Design and Enforcement Challenges (2024) (analysing regulatory uncertainty, delegated legislation, and the need for sector-specific guidance under the DPDP framework), https://vidhilegalpolicy.in

[77] Law Commission of India, Regulatory Reform and Delegated Legislation in Emerging Technology Laws (2023) (emphasizing the role of clear executive and sector-specific guidelines in reducing compliance uncertainty under new statutory regimes), https://lawcommissionofindia.nic.in