INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 2 | Issue 2 [2024] | Page 282 - 293

UNRAVELING THE DYNAMICS OF DATA PROTECTION IN M&A DUE DILIGENCE UNDER INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

- **SHAILJA SINGH**[1]

ABSTRACT

Data is the new lifeblood of a modern economy. Owing to this digital revolution, the importance of data has transcended the confines of technology-driven business and has diversified its impact across a multitude of sectors, thereby fundamentally transforming the way businesses operate and interact. The profound significance of data underscores the need for businesses to establish a data protection framework that delicately balances the preservation of client privacy and the safeguarding of their competitive edge. Hence, the enactment of the Digital Personal Data Protection Act, of 2023. As the Act exempts application of its core provisions to tribunal-approved schemes of merger & acquisitions, this effort to protect personal data by the Indian legislature extends to the continuous data transfer phase of a merger & acquisitions transaction i.e., during the due diligence stage, where the absence of robust data protection measures poses a substantial risk of data breaches and such breaches not only jeopardize the security of data but also have detrimental consequences for both the involved companies and the rightful owners of the data. While businesses grappled with regulations from the EU and the USA, the urgent requirement for India-specific legislation became evident after the pronouncement of the historic Puttaswamy Judgement. The exclusive legislation aims to instil greater accountability in companies, addressing areas that had remained largely unchecked, making it crucial to thoroughly analyse the compliance and impact of this legislation, especially in such a process that entails constant data exchange i.e., the phase of due diligence of data of the merging/acquired company. The Act mandates businesses to implement a structured framework for lawfully collecting and processing personal data from clients, employees, and others, ensuring consent, security, and reasonable safeguards against data breaches. This paper analyses the application of India's data protection legislation in the due

[1] Final year B.A. LL.B. student, Vivekananda Institute of Professional Studies.

diligence phase of an M&A transaction—a pivotal stage characterized by the extensive exchange of personal data crucial for the successful completion of the deal.

INTRODUCTION

The landmark judgment of *Justice K. S. Puttaswamy (Retd.) vs Union of India*[2] gave path to the recognition of the 'Right to Privacy', including Digital Privacy. This marked the beginning of a struggle spanning over half a decade for the implementation of a data protection law in India. The culmination of this effort occurred on August 11, 2023, with the President of India granting assent to the Digital Personal Data Protection Act, 2023 ("The Act"). The Act was imperative due to the increasing value of data in this ever-evolving digital world.

The impact of its implementation extends beyond specific domains within the corporate world, as the act comes into play wherever personal data is involved. One such area is the due diligence process during a Merger and Acquisition ("M&A") transaction. This process aids the acquiring entity in making informed decisions about the deal. It entails the continuous transfer of personal data belonging to employees, vendors, and customers of the target company from the seller to the buyer, thereby necessitating the implementation of the Act in the process. This is what exactly is dealt in this paper, i.e., the compliance of the newly-enacted Data Protection law of India in the sharing of personal data during the due-diligence phase of an M&A transaction.

The paper is organized into six sections: Part I delves into the necessity and role of data protection in due diligence. Part II elucidates the nature of data and the diverse roles entities and individuals assume during data transactions. Part III scrutinizes exemptions in M&A scenarios, prompting legal discussions on the timing of data sharing in due diligence. Part IV focuses on the current consent framework and the scope of 'certain legitimate use,' particularly in the context of employee data transfer. Parts V and VI outline the general duties of parties involved in data transactions and the redressal mechanism for their non-compliance.

I. INCREASING ROLE OF DATA PROTECTION IN DUE DILIGENCE DURING A M&A TRANSACTION

Privacy concerns are being increasingly scrutinized while going through the process of due diligence in an M&A transaction. This process involves careful examination or audit of a potential

[2] (2017) 10 SCC 1, AIR 2017 SC 4161

investment or product encompasses a thorough review of all pertinent facts, including but not limited to financial records and personal data of employees, vendors, etc., associated with the target company. 'Personal data' extends from employees' details stored in a data room to past search queries to user's IP addresses and his location. Even in conventional transactions, where personal data may not constitute an essential element of the seller's business, the captured and processed data is expected to entail data such as employment contracts, behavioural data, details regarding disputes, and significant contracts with suppliers. Buyers, in particular, concentrate on assessing both the value and potential risks inherent in the data assets possessed by the seller.[3]

One of the identifiable reasons behind why data protection is necessary in due diligence is a must is that data is the most valuable asset a company can possess and ensuring its protection and security is pertinent for both target and acquirer for safety purposes.[4] Further, the digitalisation of businesses and industries coupled with the growing prominence of intangible assets within a target company, is expected to amplify the role and significance of data protection.[5] This disclosure of personal data has number of risks associated with it, for instance disclosure of such personal data which is inadequate or excessive may hinder the due diligence process and breach the privacy of the employees, clients etc.[6]

II. NATURE OF DATA AND ROLES INVOLVED

Before delving into the nuances of how in the ever-evolving digital landscape, data protection and the process of Mergers and Acquisitions ("M&A") are intersected, it becomes pertinent to identify the specific data affected by the DPDP Act in this convoluted process. The intent of the legislation was to restrict the applicability only to processing of such personal data within India, which is either collected in digital form or is converted to digital form following the collection in non-digital form[7]. However, for data processed outside India, the Act applies when connected to activities

[3] Norton Rose Fulbright 'Privacy and Cybersecurity Due Diligence Considerations in M&A Transactions' (Data Protection Report, 24th October 2022) < https://www.dataprotectionreport.com/2022/10/privacy-and-cybersecurity-due-diligence-considerations-in-ma-transactions/ > accessed at 16th November, 2023

[4] Bianca Marcu, 'Mergers and Acquisitions and Data Protection- What you need to know' (Greenbook, July 6, 2020) < https://www.greenbook.org/insights/mergers-acquisitions-and-data-protection-what-you-need-to-know> accessed at 16th November, 2023

[5]Dr. Benjamin Fehr and Susanne Hofmann, 'Data privacy law: a critical factor for M&A transactions' (PWC, November 2018)<https://www.pwc.ch/en/publications/2018/Data%20privacy%20law_Flyer_A4_EN_web.pdf > accessed at 16th November, 2023

[6] Daniel Ilan, Cleary Gottlieb Steen & Hamilton LLP, 'Privacy in M&A Transactions: Personal Data Transfer and Post Closing Liabilities' (Harvard Law School Forum on Corporate Governance November 10, 2016) < Privacy in M&A Transactions: Personal Data Transfer and Post Closing Liabilities (harvard.edu)> accessed at 21st November, 2023

[7] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) s 3(a)

related to offering goods or services to Data Principals within the territory of India, emphasizing processing rather than mere collection. Therefore, during the due-diligence stage, the personal data being shared by the target must fulfil the requirement of being digitized, in order to attract the provisions of this Act. Moreover, the personal data of employees, vendors, clients, and other stakeholders associated with the target company should not be processed for any personal purposes. Adding to that, is imperative that neither the Data Principal nor any other individual, obligated by laws in force in India, discloses or causes the disclosure of this personal data to the public.[8]

The process of due diligence entails sharing of an extensive array of data by the acquirer for the purpose of keen assessing of the target business. The matter intensifies, particularly in case of companies whose primary business is concerned with data itself or where an M&A transaction is solely driven by the value of the data, thereby positioning digital data as a key asset in the deal.[9] In this stage, when the target company shares personal data of third parties, it may assume the role of a Data Fiduciary. 'Data Fiduciary' defined under the Act presupposes the same role as of 'Data Controller' in EU's General Data Protection Regulation ("GDPR"). It has been defined as someone who determines the purpose and means of processing of personal data, either alone or in conjunction with other persons.[10] On the other hand, the concerned parties such as employees, vendors, customers etc of the target company will step into the shoes of Data Principal, as individuals to whom the personal data relates.[11]

Upon assuming the role of Data Processors, acquirers and investors are entrusted with the responsibility of processing the third-party personal data shared by the target. However, this entrustment is to be implemented by negotiating a robust contract between the target and the acquirer, which entails the compliance of establishing reasonable security safeguards to prevent personal data breach where the data is processed by the Data Processor[12] (acquirer) by the target, strict non-disclosure mandates obligatory erasure of data, when required by law[13] and clarifying the data processing activity, including performance standards.[14]

---

[8] *Id.* s 3(b)
[9] Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra, 'Personal Data Protection in the Context of Mergers and Acquisitions' (Global Data Review, 8 April, 2022) < Personal Data Protection in the Context of Mergers and Acquisitions - Global Data Review > accessed at 14th November, 2023
[10] *Id.* s 2(i)
[11] *Id.* s 2(j)
[12] *Id.* s 8(5)
[13] *Id.* s 8(7)(b)
[14] Deborshi Bharat, 'Contractual Arrangements Under India's New Data Protection Law: A Data Fiduciary's Guide to the Data Processing Universe' (S&R Associates, 4 October 2023) < https://www.snrlaw.in/contractual-

III. EXEMPTED M&A SCENARIOS

The Act provides for certain exemptions and clarifies that the provisions of Chapter II, except sub-sections (1) and (5) of Section 8, and those of Chapter III and Section 16 referred to as "Identified Provisions" shall not apply in certain scenarios[15] and one of them is in case of a scheme of compromise or arrangement or merger or amalgamation of two or more companies or reconstruction by way of demerger or transfer or division of one or more companies. However, the key point is that such various schemes of M&As must be approved by a court or tribunal or other authority competent to do so by any law for the time being in force.[16]

Given that the Act necessitates such approval for claiming exemptions, the Identified Provisions will become applicable in alternative M&A scenarios. As an example, the processing of Personal Data during a share purchase transaction does not necessitate approval from a court or a competent authority.[17] Since the process of due diligence involves specific inquiry, gathering and verification of data received by the target company and occurs prior to the stage where parties finally decide to sign a formal contract and approval of any court or tribunal is sought, as a result any sharing of digital personal data during the process of due diligence is not to be exempted under any provision outlined in the Act. The interpretation may potentially become a subject of legal discussion in future, wherein the involved parties may find it necessary to affirm that the sharing of personal data transpired as a part of the due diligence process and not subsequent to the approval of the courts or tribunal.

IV. CONSENT PROVISIONS

GROUNDS FOR PROCESSING

It has been established till now which stage of an M&A transaction is impacted by the present legislation. The target company while sharing the personal data takes upon certain obligations under Chapter II of the Act. The company, acting as Data Fiduciaries, is authorized to process the data of third parties based on two primary grounds. Firstly, when the concerned parties have

arrangements-under-indias-new-data-protection-law-a-data-fiduciarys-guide-to-the-data-processing-universe/> accessed at 15th November, 2023

[15] *Id.* s 17(1)

[16] *Id.* s 17(1)(e)

[17] Ajay G Prasad and Nayonika Sinha, 'Impact of the Data Protection Law on Mergers & Acquisitions and Corporate Restructurings' (JSA Law, 24th August, 2023) < https://www.jsalaw.com/newsletters-and-updates/impact-of-the-data-protection-law-on-mergers-acquisitions-and-corporate-restructurings/ > accessed at 15th November, 2023

provided consent for the data processing. Secondly, when the purpose of data processing falls under 'certain legitimate uses,' even in the absence of consent. In both scenarios, it is imperative that the processing is unequivocally directed towards lawful purposes.[18] Where the consent is the ground for processing, such consent shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action.[19] Typically, the disclosure of data from the seller to the acquirer occurs during the due diligence process. Therefore, it is crucial to ascertain and fulfil consent requirements at this stage. Prior to the enactment of this Act, Privacy Rules 2011[20] governed the process of obtaining consumer consent before the use of their data. These rules have been omitted by the Act.

It is important to note that where the consent has been taken for a specific purpose, the processing must be limited for that specified purpose only.[21] For instance, if the target company has obtained consent from its vendors to share certain personal data for specific purposes, the acquiring company must ensure that any processing of this data is confined to the agreed upon purposes. If the acquiring company intends to use the vendor-related data for additional purposes beyond what was initially consented to, it could potentially lead to legal and compliance issues. Adhering to this principle of purpose of limitation, privacy rights of these third parties (Data Principals) can be more efficiently protected.

The Data Principals are free to withdraw their consent at any time where the consent serves as the basis of processing of the personal data.[22] However, the consequences of such withdrawal have to be borne by the Data Principal only and the said withdrawal shall not impede the legality of processing personal data based on consent that occurred prior to its retraction.[23] Therefore, where an employee retracts her consent, she might face challenges in terms of integration into the acquiring company's systems or processes, and her data may no longer be used for ongoing assessments or planning. However, the acquiring company can still depend on the legality of the processing actions taken during due diligence based on the initial consent, even if that consent is later withdrawn. But the Act makes it compulsory for the company to cease the processing of the personal data, within a reasonable time, on such withdrawal unless required by law.[24]

---

[18] *Id.* s 4
[19] *Id.* s 6(1)
[20] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
[21] *Id.* at 16
[22] *Id.* s 6(4)
[23] *Id.* s 6(5)
[24] *Id.* s 6(6)

The Act also provides for the appointment of Consent Managers, through which the Data Principals can manage, withdraw or review their consent.[25] However, whether these managers are mandatorily required to be appointed or are required only in special circumstances depends upon the rules prescribed by the law.[26]

NOTICE COMPLIANCE

Whenever a request for consent has been initiated by the target company to third parties, it is compulsory for them to provide, along with such request, a notice.[27] Such notice must inform the customers, employees etc. which personal data and the clear purpose for which it is to be processed by the target and the manner in which the parties may exercise and make complaint to the Data Protection Board of India established under Chapter V of the Act. In light of the recent enactment of the Act and the historical prevalence of M&A transactions over the years, the legislation accommodates situations where consent was granted prior to the Act's commencement. In such cases, the merged or amalgamated entity is obligated to expeditiously provide notice to the Data Principals, as soon as reasonably practicable.[28] The target is required to provide the Data Principals with the choice to access the contents of the notice in either English or any language specified in the Eighth Schedule to the Constitution.[29] In the context of a slump sale, wherein a specific business acquires assets, liabilities, and employees on an 'as-is' basis for a lump-sum consideration, the processing of personal data following the sale would still be subject to the provisions governing consent.[30] The breach of the provision would attract a penalty, which may extend to fifty crore rupees.[31]

CERTAIN LEGITIMATE USES

The complex process of due diligence encompasses the transfer and handling of diverse data types, necessitating the establishment of a robust consent framework, but the Act lays down 'certain legitimate uses' where the processing of the data may occur without the consent of the Data

[25] *Id.* s 6(7)
[26] Aparna Gaur and Varsha Rajesh, 'India: Exploring the practical implementation of consent managers under the Digital Personal Data Protection Act, 2023' (One Trust Data Guidance, October, 2023) <https://www.dataguidance.com/opinion/india-exploring-practical-implementation-consent#:~:text=Under%20the%20Act%2C%20a%20consent,%2C%20transparent%2C%20and%20interoperable%20platform. > accessed at 19th November, 2023
[27] *Id.* s 5(1)
[28] *Id.* s 5(2)
[29] *Id.* s 5(3)
[30] *Id.* at 14
[31] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023), Sch, Sl. No. 7

Principal. It has been made so, as such uses includes 'lack of objection' from the principal, essentially mirroring the provision of 'deemed consent' made in earlier bills of the Act, albeit with a terminological modification.

Among the eight legitimate uses, 'employee data transfer' stands out as especially important for the due diligence process. [32]This indicates that the employees' personal data can be processed even without her consent by the employer given the data is being used for:

a) The purpose of employment of the Data Principal.
b) Safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, and/or classified information.
c) Provision of any service or benefit sought by a Data Principal who is an employee.

The provision is already encompassing a broad mandate, by largely covering all scenarios in which an employee's data can be transferred by explicitly stating the 'purpose of employment'. However, a crucial question emerges: should the requirement of providing a notice to the employee be waived when sharing their data? The Act remains silent on this issue. Nevertheless, considering the principles of the Right to Privacy and Right to Life as emphasized in Article 21 of the Constitution of India, providing notice serves as a means of transparency. The omission of such notice may potentially undermine the primary objectives of the Act. The employees have the right to be adequately informed about the transfer of their personal data. Such transparency is essential to facilitate a collaborative approach and enables awareness of potential implications on their employment such as change in their working conditions, responsibilities etc., thereby, providing them an opportunity to make informed decisions regarding their employment.

V. GENERAL DUTIES OF THE PARTIES INVOLVED IN THE PROCESS OF DUE DILIGENCE

The Act is formulated is a manner that imposes a range of obligations on the Data Fiduciary, outlining specific responsibilities and duties that must be adhered to. One of the primary obligations incumbent upon the target company while transferring data to the buyer is the rigorous compliance with the provisions of the Act and the rules made in respect of processing of the data,

[32] *Id.* s 7 (i)

either done by itself or by the buyer or investors, on its behalf.[33] This duty remains obligatory notwithstanding any contractual agreements to the contrary or any shortcomings in the discharge of duties by the Data Principal as specified under the purview of the Act.[34] Another duty of the seller is to protect the personal data in its possession by establishing reasonable security safeguards to prevent personal data breach[35] The seller may take these steps through sharing such data by implementing appropriate non-disclosure agreements or through a secure platform, such as an encrypted virtual data room (VDR), which ensures limited and controlled access[36]. For example, instead of providing the buyer with detailed individual client contracts that might include confidential information about each client, the company is advised to share a standardized template or a redacted version of the agreement. This way, the necessary information for the buyer to evaluate the client relationships is provided without exposing specific and potentially sensitive details about individual clients. Through this, the company aims to maintain the confidentiality of client details while still providing the buyer with the necessary insights into the overall structure and terms of client agreements. The breach in observing this particular obligation attracts penalty which may extend to ₹ 250 crores.[37] The observance of these two obligations continues to persist even after the scheme of M&A is approved by the court/tribunal i.e., post-closing period.

Other obligations include engaging or involving the buyer/acquirer to process data on its behalf only under a valid contract[38], to implement appropriate technical and organisational measures[39], to establish an effective mechanism to redress the grievances[40] and to intimate the Data Protection Board of India in the event of any personal data breach[41]. The act of non-observance of such intimation to the Board leads to a penalty up to ₹200 crores.[42] Either on the completion of the M&A process or on the withdrawal of the consent of the clients etc., whichever is earlier, the seller is compulsorily required to erase or cause to erase the personal data, unless such retention is necessary for compliance of any law.[43] The same could be complied by ensuring the implementation of a 'Data Retention Policy' while collecting personal data.

---

[33] *Id.* s 8(1)
[34] *Id.*
[35] *Id.* s 8(5)
[36] Bianca Lewis and Jessica B. Lee 'Data Privacy and Security Considerations in M&A Transactions' (Loeb & Loeb LLP, February 2022) < https://www.loeb.com/en/insights/publications/2022/02/data-privacy-and-security-considerations-in-ma-transactions > accessed at 21st November, 2023
[37] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023), Sch, Sl. No. 1
[38] *Id.* s 8(2)
[39] *Id.* s 8(4)
[40] *Id,* s 8(10)
[41] *Id.* s 8 (6)
[42] *Id* Sch. Sl. No. 2
[43] *Id.* s 8(7)

These obligations of the sellers become the rights of the Data Principals and apart from these, Chapter III of the Act highlights the specific rights of the subjects. Firstly, the Data Principal, having granted consent, can request information from the target, this includes a summary of processed personal data, details of processing activities, identities of other involved entities, and additional prescribed information.[44] Adding to that, they have the right to correct/complete/update the inaccurate/incomplete personal data[45] and to nominate any other individual who will exercise her rights in the event of death or incapacity.[46]

However, in line with what Harold Laski rightly said "***one man's right is also his duty***", some duties have also been imposed on these owners of the personal data. Notably, these are attributed to them majorly at the time of collection of data rather than at the time of due diligence process where data is being processed. An employee, business representative, or client is obligated not to impersonate another individual and must refrain from withholding any material information pertaining to proof of identity or proof of address while submitting personal data. The obligation is to provide only information that is demonstrably authentic and verifiable.[47] Therefore, even if the data principal does not have any direct duty to perform in the process of due diligence, they are compelled to undertake these duties beforehand so as to safeguard the future interests of the merger or acquiring company. Failure to do so may result in a significant setback, as exemplified in the 2017 Verizon-Yahoo! deal, where Verizon identified a cybersecurity issue after entering into an acquisition agreement with Yahoo![48]

VI. GRIEVANCE REDRESSAL PROCESS IN CASE OF PERSONAL DATA BREACH

The consequences and the risks involved in personal data breaches severally attack not only the companies but also the owners of such personal data. One of the most prevalent issues that frequently arise during the due diligence process involves challenges associated with accessing such policies or engaging with such personnel who are responsible for ensuring the security and privacy

[44] *Id.* s 11
[45] *Id.* s 12
[46] *Id.* s 14
[47] *Id.* s 15
[48] Richard D. Harroch, Jennifer Martin, and Richard V. Smith, 'Data Privacy and Cybersecurity Issues In Mergers And Acquisitions' (Forbes, November 11, 2018) <https://www.forbes.com/sites/allbusiness/2018/11/11/data-privacy-cybersecurity-mergers-and-acquisitions/?sh=68d5a0f872ba > accessed at 20th November 2023

of collected personal data.[49] For this reason, the Act has provided a multi-layered right to grievance redressal to the Data Principals which enables them to access the redressal mechanism provided by the target company or the appointed consent managers.[50] The company or the appointed consent manager is required to respond to the grievances within the prescribed time limit,[51] simultaneously, the Data Principals are empowered to redress their grievances at the Data Protection Board of India (DPBI). However, such recourse to the Board is permissible only after exhausting all available avenues for redressal.[52]

In the due diligence, it is imperative for a data fiduciary to diligently protect the personal data within its purview, including data handled by the buyer. This necessitates the implementation of reasonable security measures to mitigate the risks of unauthorized processing. In the case of any breach, irrespective of its magnitude or the nature of the data involved, the data fiduciary is obligated to expeditiously inform both the Data Protection Board of India (DPBI) and each impacted data principal.[53] Following such receipt, the DPBI holds the authority to prescribe urgent remedial actions, conduct thorough inquiries into the breach, and enforce penalties as deemed necessary.[54]

DPBI comprises persons who possess special knowledge or practical experience in the fields of data governance[55] and have the power of a civil court.[56] Upon receiving a complaint, the Board will assess whether there are sufficient grounds to initiate an inquiry.[57] In cases where no grounds are identified, the Board has the discretion to conclude the proceedings, duly recording the reasons for such closure[58]. However, if the Board determines the sufficiency of grounds, it will proceed with a thorough inquiry. This process will include affording the concerned parties a fair opportunity to be heard, adhering to principles of natural justice, and imposing the necessary

[49] Christopher M. Caparelli, Winnie Hu and Alessandra (Ali) Harkness, 'Privacy and data security due diligence: The importance of implementing post-closing improvements' (Torys LLP, 2023) <https://www.torys.com/en/our-latest-thinking/publications/2022/04/privacy-and-data-security-due-diligence > accessed at 21st November, 2023
[50] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023), s 13(1)
[51] Id. s 13(2)
[52] Id. s 13(3)
[53] Id. s 8(6)
[54] Id. s 27
[55] Id. s 19(3)
[56] Id. s 28(7)
[57] Id. s 28 (3)
[58] Id. s 28(4)

penalties[59], up to ₹250 crores. The Board, to the extent feasible, will function as a digital office and implement the requisite techno-legal measures accordingly.[60]

The Board may also direct the path of mediation to the concerned parties[61]. A novel concept introduced in the 2023 Act, different from what earlier Bills of the Act had, is the concept of 'voluntary undertaking', where the offending company may voluntarily undertake future compliance and the acceptance of such undertaking will be regarded as a bar on further proceedings and lastly, failure of adherence to the terms will be deemed to be a breach[62]. Adding to that, an appeal can be lodged against DPBI's orders within 60 days before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).[63]

CONCLUSION

In the M&A due diligence process, there is a continuous exchange of data from the seller to the buyer, encompassing the personal information of employees, clients, and business representatives. Safeguarding this data is essential to uphold the privacy rights of the individuals concerned. Recognizing this need, the implementation of data protection legislation became vital. Consequently, the Digital Personal Data Protection Act 2023 was enacted to establish a robust framework that facilitates the processing of such data in a secure and privacy-conscious manner. The Act mandates entities to institute a consent and notice provision, ensuring transparency in the process of legally sharing data by obtaining the consent of the owner of the personal data. Under the provisions of the Act, companies are mandated to implement reasonable safeguards to mitigate the risk of data breaches. Consequently, the Data Protection Board of India is empowered to levy penalties on entities that fail to uphold these safeguards.

[59] Id. s 28(6)
[60] Id. s 28(1)
[61] Id. s 31
[62] Id. s 32
[63] Id. s 29