FIDUCIARY DUTIES IN THE DIGITAL AGE: A CRITICAL EXAMINATION OF THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

Manasa Ravi & Ishaan Porwal, OP Jindal Global University

ABSTRACT

With the advent of new digital age in India, the requirement to formulate laws governing its use also emerged: the Digital Personal Data Protection Act 2023 (DPDP Act). This article examines in detail the purpose and elements of the Act, which seeks to regulate personal and sensitive data. The ambitious Act is faced with multiple challenges that may undermine its goals, including high levels of opacity, limited measures available for people whose data is collected and processed, certain categories of data being incompletely addressed and room for arbitrary government intervention. The discussion explains how these problems contribute toward an instance of agency problem where the data fiduciaries act against the persons whose data they collect and process. The article also assesses the DPDP Act in relation to the the General Data Protection Regulation (GDPR) of the European Union which is considered the standard of data protection laws across the world. While the DPDP Act heavily derives from these regulations and is symmetrical in multiple aspects, it does not measure up to the GDPR in the dimension of the extent of coverage, breach notification, and accountability of the offenders. This highlights multiple areas of improvement for the newly introduced act. In addition, the research emphasizes the importance of extending comprehensive fiduciary responsibilities to data handlers in order to conduct business without impinging on the rights of data principals. It calls attention to the need for the establishment of clear policies coupled with enforcement mechanisms to mitigate these agency issues. Finally, this article seeks to provide ways to improve the DPDP Act to make it more clear, responsible, and equitable.

INTRODUCTION

India, along with the global economy, has been undergoing rapid digitalisation in the past three decades. Along with the numerous benefits that have been relished, the concerns regarding data security and data privacy have been persistent. The public has been more conscious of the possible hazards and vulnerabilities associated with their information as a result of the extensive collecting, storage, and use of personal data brought about by the increased use of technology.[1] This has generated an acute need for development of laws to govern the digital realm.

India has responded to this necessity with the introduction of The Digital Personal Data Protection (DPDP) Act in 2023, aiming to control the way personal details are handled within the digital space, with a focus on creating a secure ecosystem for online interactions.[2] The primary challenge to creating security lies in curbing business activities that monetise on the lack of these measures. This raises the requirement for imposing fiduciary duties on the firms, ensuring their interests align with the individuals whose data they manage.

This article aims to analyse the Digital Personal Data Protection Act 2023's effect on securing individual's data from potential exploitation from the data handlers by identifying gaps in the legislation that could hamper the process and suggest recourses to resolve them.

This article begins with recognising the development of the legislature. Further, the agency problem that need to be addressed are evaluated. Thirdly, the Data Protection Act is analysed and shortcomings are examined, which is also evaluated alongside European Union's General Data Protection Regulation. Fourthly, the impact of Government intervention which poses an adversity for both the company as well as the data principles are explored. Additionally, the Act's relevance in the judicial sphere is studied. Finally, the article concludes with suggestions derived from these observations to create a just and accountable digital ecosystem.

---

[1] Antima Tiwari, 'A PARADIGM SHIFT IN DATA PROTECTION: ANALYZING THE DIGITAL PERSONAL DATA PROTECTION BILL IN THE CONTEXT OF INDIA'S PRIVACY LANDSCAPE ARTICLES' (2023) (*Manupatra*, 22 September 2023) <https://articles.manupatra.com/article-details/A-Paradigm-Shift-In-Data-Protection-Analyzing-The-Digital-Personal-Data-Protection-Bill-In-The-Context-Of-India-s-Privacy-Landscape> accessed 2 February 2025.

[2] Ajay Kumar Bisht, and Neeruganti Shanmuka Sreenivasulu. 'Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023.' (2024) *Data Privacy-Techniques, Applications, and Standards*, IntechOpen.

DEVELOPMENT OF THE DIGITAL PERSONAL DATA PROTECTION BILL 2023

India has taken significant steps to create a holistic data protection regime over the years. This was initiated with an amendment to the Information Technology Act, 2000 (IT Act) in 2008, where Section 43A was introduced, obligating companies to implement security practices for digitalized personal data.[3] In 2011, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules) was introduced with further regulations for protection.[4] Nonetheless, India did not have substantive laws that kept pace with the rapid digitalization, which was flagged in 2017 by the Supreme Court in K.S. Puttaswamy v. Union of India.[5] The landmark judgement held privacy to be a fundamental right under Article 21 of the Constitution, and also highlighted the State's duty to protect and regulate privacy of individuals. Furthermore, the punishment was a fine extending to merely Rs. 5,00,000 or imprisonment for up to 3 years,[6] calling for a more serious approach to data protection laws and holding the data fiduciaries liable. This remarked the beginning of establishing a comprehensive data protection law in the country.

Following the recommendations of the nine-judge bench, the Sri Krishna Committee[7] was formed, and in 2018, it released the Draft Personal Data Protection Bill. This bill, and multiple others developed subsequently, were tabled by The Ministry of Electronics and Information Technology (MeitY). India's six-year-long efforts bore fruit with the introduction of the final bill by MeitY in August 2023, which has been enacted as The Digital Personal Data Protection Act, 2023,[8] comprising the intensely researched, scrutinised, and developed data protection laws. This has replaced the previously prevalent laws regarding the subject under The IT Act and The SPDI Rules.[9] This marks the end of India's journey towards developing the paramount laws regarding digital data, showcasing its commitment to safeguard individuals in the newly digitalised world. However, the question of how effectively companies can implement these measures while balancing the incentives to monetize data remains unresolved.

---

[3] The Information Technology Act 2000, s 43(a).
[4] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.
[5] *K.S. Puttaswamy v. Union of India* (2017) 10 SC 1.
[6] The Information Technology Act 2000, s 33(2)
[7], Vrinda Bhandari and Renuka Sane, 'Protecting citizens from the state post Puttaswamy: Analysing the privacy implications of the Justice Srikrishna Committee Report and the Data Protection Bill' (2018) 14 Socio-Legal Rev 143.
[8] The Digital Personal Data Protection Act 2023.
[9] The Digital Personal Data Protection Act 2023, s 44(2).

AGENCY PROBLEMS IN IMPLEMENTING DATA PROTECTION MEASURES

The need for a transformation in the digital economy is cardinal as e-commerce is flourishing and any business, irrespective of its size, nature or collect sensitive private information that need to be safeguarded. With the growing advantages of technology, the drawbacks are inevitable, which include increasing hacking into databases, causing breaches. In 2024, six months alone had "388 data breaches, 107 data leaks, 39 ransomware group activities and 59 cases of access sales or leaks" recorded cases in India.[10] These cause immense financial burden on the company. The RBI estimated around reached $2.18 million losses in 2023, showcasing the gravity of the issue.[11] Further, there is also severe long-term reputational harm that result after such breach, visible through the falling stock prices due to loss of investor confidence and falling revenue due to loss of costumers.[12]

While this indicates that firms should willingly adopt the strongest data protection measures, their focus rests on protection of the data they own rather than protecting the privacy of the data principals. This is due to the numerous advantages a firm gains from monetising on the data collected. It helps firms turn raw information into a valuable assets and that brings in new revenue streams, aid with decision making and overall increase operational efficiency on all aspects.[13] The competitive advantage this brings in is highly desirable and firms are inclined to undertake this approach. The common phrase "If you are not paying for it, you are the product"[14] sheds light on the ethicality concerns of such practice, forming the basis for restrictions placed by the data protection laws.

This represents the company's dilemma in adopting strategies for data collection and processing as on one hand they benefit immensely from its usage but also risks being vulnerable to severe financial, reputation and legal costs if costumers believe their data is unethically collected or misused along with the concerns regarding security breaches. Additionally,

[10] BL Kochi Bureau, 'India Breach Report: 593 Cyber Attack Cases in H1 of 2024' (*BusinessLine*, 30 July 2024) <https://www.thehindubusinessline.com/info-tech/593-cyber-attack-cases-reported-in-h1-of-2024-india-breach-report/article68463278.ece> accessed 2 February 2025.
[11] Reserve Bank of India, *Report on Currency and Finance 2023-24* (RBI 2024).
[12] Griselda Sinanaj and Jan Muntermann, 'Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis' (*AIS Electronic Library (AISeL)*, 18 June 2013) <https://aisel.aisnet.org/bled2013/29/> accessed 2 February 2025.
[13] Joan Ofulue and Morad Benyoucef, 'Data Monetization: Insights from a Technology-Enabled Literature Review and Research Agenda' (2022) 74 Management Review Quarterly 521.
[14] Scott Goodson, 'If You're Not Paying for It, You Become the Product' (*Forbes*, 12 October 2022) <https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/#2f702eac5d6e)> accessed 2 February 2025.

conflict of interest between different parties, termed as agency problem, is in interplay here. One of the problems involve the conflict between the firm itself and the other parties with whom the firm contracts, such as creditors, employees, and customers, which displays the apprehension of the firm, as an agent, behaving opportunistically and exploiting the principals.[15] This underscores the importance of having data protection laws that curb all possibilities of exploitation, urging the companies to adopt ethical data usage practices, which would benefit both the parties involved. The DPDP Act aims to address these issues but falls short in certain respects, these shortcomings need to be explored to the understand the viability of the new law.

ANALYSIS OF DIGITAL PERSONAL DATA PROTECTION ACT 2023

The Digital Personal Data Protection Act 2023 aims to create a haven for digital transactions, eliminating the agency problem concerned. However, the law lacks clarity and provides room for loopholes in certain aspects that can be misused to deviate from the objective of the Act. Firstly, there is a lack of transparency that allows for exploitation of data beyond the knowledge of the holders. Secondly, the Act provides various rights to the data principals but lacks in the adequate implementation of them, allowing for an opportunity to exploit these areas and not secure them the rights. Thirdly, the protection is not extended to all forms of data, creating a passage for further unethical usages.

(i) Lack of transparency

Guidelines regarding notice for collection of data has not been formulated in accordance with the definitions of consent[16] which requires it to be "specific, informed, unconditional and unambiguous"[17] In the previously rejected bills, there were inclusions of informing the data principals regarding the duration of collecting data, disclosing the sharing with third parties as well as the international transfers of the data, which has not been incorporated in the 2023 Act. The Section 5 of DPDP Act[18] which elaborated on the contents of the notice focuses merely on the purpose, falling short in meeting the standard of informed consent.

[15]John Armour, Henry Hansmann and Reinier Kraakman, 'Agency Problems and Legal Strategies' (2017) The Anatomy of Corporate Law 29.
[16] The Digital Personal Data Protection Act 2023, s 5.
[17] The Digital Personal Data Protection Act 2023 s 6.
[18] The Digital Personal Data Protection Act 2023, s 5.

Section 7 of the DPDP discusses the ambit of consent but the it involves lack of transparency, which cannot be overlooked. It provides a conclusive list of legitimate uses but sub-section (a) reads "of which she has not indicated to the Data Fiduciary that she does not consent to the use of her personal data"[19] to establish prohibited actions by the entity collecting the data, which can be construed as vague. This clause places the burden entirely on the data principal to establish the limits of the usage, and does not hold the company liable. The latter is not obligated to reveal the details of the data processing, but rather merely state the purpose while obtaining consent. These purposes can be construed as widely as possible and the data principals would be oblivious to the misuse.

For instance, a company's collection of data of employees for purposes of employment can be observed to gain an insight on the gaps this clause creates. The company could subsequently share employees' data with third-party partners for marketing of the company's own products, claiming internal marketing to be part of the company's broader strategy to improve employee morale, which could loosely be tied to employment. As per Section 7, if the employee does not specifically withdraw consent for this purpose, the firm can exercise its right to use the data, ignoring the concerns of the employee for its own benefits, escalating the agency problem. According to the law, if it provides transparency of the processing to all the data principals, they can exercise their right to withdraw consent if required and their interests will not be side-lined by masking their activities.

Without clearly defined obligations for data fiduciaries, the burden of responsibility shifts disproportionately to data principals, complicating their ability to protect their own data. This lack of specificity only perpetuates the agency problem as the firm's liability of aligning its works in the principal's interests is reduced.

(ii) Lack of recourse for exercising rights

One of the main criticisms of the DPDP Act is that it acknowledges the data principal's right, but does not yet provide sufficient recourses regarding its exercise.[20] The "right to be forgotten" reflects the claim of an individual to have certain data deleted so that third persons can no

[19] The Digital Personal Data Protection Act 2023, s 7(a).
[20] Shagun Kabra and Khyati Lad, 'Advancement Of Technology, Lack Of Privacy: Pre-Requisite Of The Digital Personal Data Protection Act, 2023.' (2024) 11 International Journal of Research and Analytical Reviews 49.

longer trace them.[21] The Puttaswamy judgement which held this right to be as an essential part of the right to privacy also highlighted the need for implementation of the same.[22] Section 12 of the DPDP Act has attempted to provide a forum for exercising this right, but it provides undue power in the hands of the data fiduciary rather than the data principal over their own personal data. The exception stating, "unless retention of the same is necessary for the specified purpose" [23] does not instil any barriers on the gravity of the purpose. It could range from a legitimate public interest to merely a business opportunity, hence, failing to impose a genuine obligation towards the erasure of such data. The Srikrishna Committee in 2018, following the judgement on privacy, noted that the right to be forgotten is a concept aiming to introduce the limitations of human memory into an otherwise boundless digital realm.[24] The vision of the committee over the control an individual has over digital footprint have not been incorporated in the Act as the ambiguous construction of it underplays the fundamental right to erasure.

The gaps in obligations is evident is Section 8(6) of the DPDP Act[25] which mandates reporting of Data Breach to the Data Protection Board, but fails in providing timeline for the same.[26] The absence of a clear deadline may encourage some Data Fiduciaries to avoid taking immediate action or delay reporting until the consequences are more severe. This undermines the spirit of accountability in data protection laws, as it allows companies to act in their own interest rather than prioritising the protection of users' data. It is the Board's responsibility to suggest remedial measures and impose restrictions, which are time-sensitive.[27] If timely notification of such breach to Data Principals remains unconsidered, it creates a vulnerable position where they are unable to take measures to protect themselves, such as changing passwords, freezing accounts,

[21] Prashant Mali, 'Privacy Law: Right to Be Forgotten in India I.' (*NLIU Law Review*, July 2018) <https://nliulawreview.nliu.ac.in/wp-content/uploads/2022/01/Volume-VII-17-33.pdf> accessed 2 February 2025.
[22] Rajat Anuprash and Gaurav Bharti, 'Right to Be Forgotten in India: A Critical Legal Analysis' (*Indian Journal of Law and Legal Research*, 4 August 2022) <https://www.ijllr.com/post/right-to-be-forgotten-in-india-a-critical-legal-analysis> accessed 2 February 2025.
[23] The Digital Personal Data Protection Act 2023, s 12.
[24] Saket Singh Sengar, 'From Pixels to Policies: Analysing the Provisions and Navigating the Complexities of the Digital Personal Data Protection Act, 2023' (*SSRN*, 25 March 2024) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4547842> accessed 2 February 2025.
[25] The Digital Personal Data Protection Act 2023, s 8(6).
[26] Sohineet Banarjeet and Anmol Bharukatt, 'Preparing for a New Data Protection Regime' (*SCC Times*, 16 February 2024) <https://www.scconline.com/blog/post/2024/02/07/preparing-for-a-new-data-protection-regime/> accessed 2 February 2025.
[27] Chanlang Ki Bareh, 'Reviewing the Privacy Implications of Indias Digital Personal Data Protection Act (2023) from Library Contexts' (2024) 44 DESIDOC Journal of Library & Information Technology 50.

or being vigilant for fraud. If the breach is reported too late, the damage to individuals could be far more significant.

The lack of recourse for exercising rights highlights agency problems as it places data fiduciaries in a position of power over data principals, allowing them to act in self-interest rather than in the interest of those whose data they collect. By failing to establish a framework that empowers individuals to enforce their rights effectively, the Act allows fiduciaries to prioritize their operational needs and business interests, often at the expense of data principals' rights and privacy. This imbalance can lead to a lack of trust in data handling practices and perpetuate a cycle of exploitation.

(iii) Lack of protection

The Act explicitly excludes "personal data that is made or caused to be made publicly available" as mentioned in Section 3(c)(ii),[28] which fails to instil trust in the digital world. Instances such as unauthorised circulation and processing of personal information shared on social media, would fall outside the purview of the act, overlooking a significant breach of privacy.[29] The focus on the consent of users which is central to the objectives of the Act is deviated by the ambiguous exception that provides room for companies to exploit a user's data evading the requirement of consent for their own purposes. This need not be informed to the users, leading to the usage in the absence of their knowledge.

The definition of personal data in Section 2(t) of DPDP Act specifies 'identifiable data', which would not encompass anonymous data. With the growing technologies, it is significantly easier to re-identify users from anonymous data, as established form a study where 90% of credit card users data was re-identified over a course of 3 months,[30] which could potentially apply to all other forms of data. The protection failing to apply to these anonymised data since it ceases to be personal according to the definitions of the DPDP Act risks the users privacy once de-

[28] The Digital Personal Data Protection Act 2023, s 3(c)(ii).
[29] MNLUM Law Review Blog, 'India's Data Protection Odyssey: A Look into the Shortcomings of the DPDP Act, 2023' (*lawreview.mnlumumbai.edu.in*, 22 October 2023) <https://lawreview.mnlumumbai.edu.in/2023/09/17/indias-data-protection-odyssey-a-look-into-the-shortcomings-of-the-dpdp-act-2023/> accessed 4 February 2025.
[30] Yves-Alexandre de Montjoye Y-A and others, 'Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata' (2015) 347 Science 536.

anonymised.[31]

Further complicating agency problems, the DPDP Act fails to adequately protect data principals from exploitation through a lack of protection. The Act permits companies to sidestep consent requirements on publicly available information and exempts anonymous data from a definition of personal data; therefore, allowing fiduciaries to operate at minimal accountability. This leniency leads to undertaking initiatives that benefit business interest than ethical treatment of the people's information.

COMPARISON WITH GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) is widely regarded as the world's most comprehensive framework for data protection.[32] It sets the standard for data protection laws, making it ideal for comparison with the DPDP Act to evaluate its effectiveness and identify areas of improvement.

(i) Scope of Protection

The GDPR involves a rather inclusive definition on what construes as 'personal data' for the purposes of enabling the protection offered under it. The concern flagged in the DPDP Act, regarding the personal data available for public is not excluded in these rules. Additionally, the GDPR's protection encompasses even offline data, an aspect overlooked by the Indian law.[33] Section 3 of the DPDP Act limits its application to personal data collected digitally or later digitized, leaving offline data unprotected.[34] This creates vulnerabilities for sensitive information collected in physical form, which can be misused without legal consequences. Additionally, the gap allows organizations to evade compliance by keeping data offline, resulting in inconsistent privacy protections.

[31] Deborshi Barat, 'It's Personal: A Roadmap for Data Mapping in Digital India' (*S&R Associates*, 22 December 2023) <https://www.snrlaw.in/its-personal-a-roadmap-for-data-mapping-in-digital-india/> accessed 4 February 2025.
[32]Matt Burgess, 'What Is GDPR? The Summary Guide to GDPR Compliance in the UK' (*Wired*, 24 March 2020) <https://www.wired.com/story/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018/> accessed 4 February 2025.
[33] Khilansha Mukhija and Shreyas Jaiswal, 'Digital Personal Data Protection Act 2023 in Light of the European Union's GDPR' (2023) 4 Jus Corpus Law Journal 322.
[34] Digital Personal Data Protection Act 2023, s 3.

The GDPR, in Articles 13, 14 and 15 elaborates on the requirements of data controllers to provide detailed information to individuals about the identity, purposes of processing, legal basis, and the involvement of third parties for both direct and indirect data.[35] It also provides transparency around data transfers and offers data principal's the right to access, correct, and object to the use of their data. The DPDP Act, however, mandates data fiduciaries to inform individuals about the specific data being processed, the purpose of processing, and mechanisms for of filing complaints, which is rather consent-based processing model, instead of the privacy centric model incorporated by GDPR, limiting the awareness.[36]

The boundaries on the extent of protection envisaged for individuals under the DPDP Act are not incorporated. The data fiduciaries as agents, may act in a way contrary to the interests of the data principals, which is not adequately protected. Evasion of protection of offline data or lack of transparency places the data principals at the risk of their trust and rights being abused by the fiduciaries, escalating the agency problem.

(ii) Breach Notification and Accountability

Article 4(12) illustrates an extensive meaning of breach, according to which any leak would constitute a breach.[37] The reporting of such breaches have also been provided with a strict timeline, with Articles 33 and 24 providing a deadline of 72 hours.[38] As discussed previously, the DPDP is yet to establish procedures for report, leaving the compliances subject to further regulations. An improved scheme is necessary to ensure accountability, which will mandate the data fiduciaries into complying with their agency duties towards the data principals.

Article 82(1) of GDPR[39] provides for data principals to receive compensation from the defaulters for both 'material' and 'non-material' damages, extending their liability to the

[35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, arts 13–15.
[36] Douwe Korff, 'The Indian Digital Personal Data Protection Act, 2023, Viewed from a European Perspective' [2023] SSRN Electronic Journal.
[37] Pimenta Rodrigues GA and others, 'Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review' (2024) 9 Data 27.
[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, arts 24, 33.
[39] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 82(1).

source.[40] Notably, this provision is absent in the DPDP Act, in fact the implementation of the act overrides section 43A of the IT Act,[41] which allowed for such compensations to victims. While companies are required to pay penalties, this does not directly benefit the affected individuals. This hampers the principal-agent relationship, as customers, who bear the brunt of data breaches or misuse, receive no compensation. The lack of direct redress could leave the consumers feeling unprotected and side-lined, with the indication that their interests are not prioritized, eroding trust in the long run.

(iii) Processing Children's Data

An organised method to protecting children's privacy is offered by the GDPR, which requires parental agreement before processing personal data belonging to kids under the age of 16.[42] Additionally, it gives member nations significant leeway in lowering this age limit. However, the DPDP Act takes a more stringent approach, outlawing behavioural monitoring, profiling, and targeted advertising for minors, with the aim to shield children from potentially dangerous data activities.[43] Furthermore, GDPR focuses more on the processing of the children's data[44] whereas the DPDP Act focuses more on the verifiable consent of parents.[45]

According to the DPDP Act's Sections 9(1) through 9(3), processing personal data belonging to minors under the age of 18 requires parental consent. [46] Despite its apparent simplicity, this general age limit presents real-world difficulties for companies. It can be difficult to verify users' ages, particularly online, and may call for invasive data collecting techniques since the

[40] Jonas Knetsch, 'The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases' (2022) 13 Journal of European Tort Law 132.
[41] The Information Technology Act 2000, s 43(a).
[42] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 8.
[43] Ayush Verma, Associate & Aman Taneja, Principal Associate with inputs from Sreenidhi Srinivasan, Partner, *GDPR v. India's DPDPA: Key Differences and Compliance Implications*, Legal500, https://www.legal500.com/developments/thought-leadership/gdpr-v-indias-dpdpa-key-differences-and-compliance-implications/ (last visited Feb. 2, 2025).
[44] 'Data Protection under GDPR' (*Your Europe*, 1 January 2022) <https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm> accessed 10 February 2025.
[45] 'Draft Data Protection Rules Mandate Due Diligence, Explicit Consent for Processing Children Data' (*The Economic Times*, 3 January 2025) <https://economictimes.indiatimes.com/tech/technology/draft-data-protection-rules-mandate-due-diligence-explicit-consent-for-processing-children-data/articleshow/116923919.cms?from=mdr> accessed 10 February 2025.
[46] Digital Personal Data Protection Act 2023, s 9.

process of verification has not been established by the guidelines[47]. Consequently, businesses may be exposed to compliance issues as a result of uneven methods to age verification brought on by the absence of defined norms.

The DPDP Act's approach to protecting children's data poses real-world difficulties for companies, especially those in industries where children make up a sizable user base, such as social media, gaming, and ed-tech.[48] Implementing strong age verification procedures and making sure that the limitations on profiling, behavioural tracking, and targeted advertising are followed are challenges that these platforms must overcome. The rule in the draft included a tedious process to process children's data where additional to parents allowance, it required the parents to prove a parent-child relationship through documents or digital locker token.[49] This indicates the standards which would likely be accommodated which would not only make children's access to online resources difficult but also drastically affect the companies operating in India.

Section 9(5)[50] allows the Central Government to exempt businesses of the requirements for children's data protection under Section 9(1) and (3) if they are satisfied that it is 'verifiably safe', setting a rather vague benchmark. This generates a dangerous ambiguity, wherein a social media platform could claim its content moderation policies make it 'verifiably safe' for children, yet still collect and analyse their behavioural data for targeted advertising, bypassing stricter protections under the Act. To provide a high degree of security for children's personal data, the regulations must be consistently enforced by all enterprises, regardless of exemptions.[51]

The DPDP Act, through its policies regarding protection of children's data, once again strays far from its attempt to enforce fiduciary duties. Firstly, the lack of standards for verification

[47] Cyril Shroff and others, 'Children and Consent under the Data Protection Act: A Study in Evolution' (*Cyril Amarchand Mangaldas Blogs*, 22 August 2023) <https://corporate.cyrilamarchandblogs.com/2023/08/children-and-consent-under-the-data-protection-act-a-study-in-evolution/> accessed 9 February 2025.
[48] Astha Bhumish Shah, 'Implications on the Data of Children after the Enactment of Digital Personal Data Protection Act, 2023 ' (*Child Rights Clinic* , 30 July 2024) <https://jgu.edu.in/child-rights-clinic/implications-on-the-data-of-children-after-the-enactment-of-digital-personal-data-protection-act-2023/> accessed 9 February 2025.
[49] Harsh Walia and Vanshika Lal, 'India's Leap towards An Era of Privacy: Meity Releases Draft Digital Personal Data Protection (DPDP) Rules' (*SCC Times*, 28 January 2025) <https://www.scconline.com/blog/post/2025/01/28/indias-leap-towards-an-era-of-privacy-meity-releases-draft-digital-personal-data-protection-dpdp rules> accessed 3 February 2025.
[50] Digital Personal Data Protection Act 2023, s 9(5).
[51] Sohineet Banarjeet and Anmol Bharukatt, 'Preparing for a New Data Protection Regime' [2024] 2024 SCC OnLine Blog Exp 14.

ensure that there are no safeguards against instances such as fake accounts, lifting the responsibility away from the platforms. Secondly, the compliances discussed are creates a strenuous considering vast presence of children on various multinational platform whose access needs to be verified by companies. Since it is vastly different from the current norms and the GDPR, it is likely to discourage their operations in the country. This indicates a need to generate a more viable verification method that does not burden the complying company but also ensures they are diligently followed. Finally, the exemption allow for easy yet legal means to evade from the responsibility towards the consumers wherein children's data can be exploited if they can showcase certain standards of safety. The law is silent about the misuse if the standards are subsequently unmet, creating further possibilities of harm through the breach of fiduciary duties.

GOVERNMENT INTERVENTION UNDER DPDP ACT

The DPDP Act gives the Indian government the authority to drastically change compliance standards by upcoming regulations and announcements. Although this dynamic method may provide flexibility, it also adds an element of unpredictability that can make long-term planning and data protection investment more difficult.

(i) Uncertainty with Exemptions

The clauses pertaining to exemptions represent a significant area of difference. The DPDP Act's Section 17(5) gives the government the authority to exempt any company or group of companies from compliance for a maximum of five years.[52] The rule is unclear about the requirements for granting exclusions and, more importantly, the time limits on their length. The exemption provision's vagueness raises the possibility of arbitrary implementation and jeopardizes the development of an industry-wide data protection standard. When exemptions are withdrawn, businesses that depend on them may experience abrupt changes in their compliance requirements, requiring quick and expensive changes to their data processing procedures.[53] This would be in contrary to the aim of such exemptions to encourage development of industries.

[52] Digital Personal Data Protection Act 2023, s 17(5).
[53] Åke Freij, 'Regulatory Change Impact on Technology and Associated Mitigation Capabilities' (2021) 34(12) Technology Analysis & Strategic Management 1418.

Furthermore, under Section 17(2)(a), any government agency can be completely exempted from the law.[54] Section 7(b) permits the Government to collect and share data without explicit fresh consent that one may have given on another website or source[55]. The Government through these exemptions, gives itself the power to arbitrarily collect unconsented personal data of the users. The exemptions granted in a lot of provisions, comes with the wording, 'subject to such conditions, as may be prescribed'.[56] This further gives the government excessive discretion on how to use the laws and in whose favour.[57]

The various broad and vague exemptions, especially to government agencies, has given the government undue control over personal data without any safeguards or responsibilities.[58] The access of fiduciaries and the government to personal data in the name of 'national security' and 'public interest' is too vague and not in the best interests of stakeholders.[59] This may create conflict among data fiduciaries due to inequality of application of laws and eventually conflict between the fiduciaries and the government. The impact may even extend to international organizations finding it difficult to comply with laws in India, creating unsurety of the continuation of their operations within the country. Therefore, the government's powers and the exemptions of the law needs to be kept in check through methods such as the Puttaswamy Test of need and proportionality.[60]

(ii) Cross Border Data Transfer

The movement of personal data across international borders is a crucial component of data protection regulations. Since GDPR has been prevalent in international business from its inception, DPDP differing from those standards poses to be harmful for companies that are complying with both regulations. The intervention by the Government is one of the main concerns for multinational companies working in the arena.

---

[54] Digital Personal Data Protection Act 2023, s 17(2)(a).
[55] Digital Personal Data Protection Act 2023, s 7(b).
[56] Digital Personal Data Protection Act 2023, s 9(4).
[57] Anirudh Burman, 'Understanding India's New Data Protection Law' (Carnegie Endowment for International Peace, 16 October 2023) https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en accessed 4 February 2025.
[58] Ishita Khanna, 'Towards Independence and Accountability in Data Protection Governance' (2023) 10 CMET 74
[59] Khilansha Mukhija and Shreyas Jaiswal, 'Digital Personal Data Protection Act 2023 in Light of the European Union's GDPR' (2023) 4 Jus Corpus Law Journal 322.
[60] Vrinda Bhandari and others, 'An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict' (2017) 11 IndraStra Global 5.

The GDPR acknowledges the interdependence of the European market and promotes the free movement of data within the EU[61]. Standard Contractual Clauses (SCCs) and adequacy determinations[62] are two of the explicit methods it offers for international transfers through Article 46 of the GDPR.[63] SCCs guarantee a minimum degree of security for transmitted data by providing a uniform set of contractual requirements for importers and exporters of data. Adequacy decisions, on the other hand, allow for smooth data transfers to non-EU nations by acknowledging that they provide similar standards of data security. The GDPR framework's consistency and transparency make it easier to share data and conduct business internationally.[64]

However, the DPDP Act adds a level of ambiguity to cross-border data transfers. Through a notice, the government may limit the transfer of personal data to particular nations under Section 16(1).[65] Businesses functioning on a large scale, apart from complying with international norms will have to additionally safeguard data from Indian recipients separately, increasing the risk of errors. Due to this uncertainty, existing data flows may be disrupted, and expensive changes to the infrastructure for data processing and storage may be required.

Section 16(2) adds to this uncertainty by giving the government the power to restrict cross-border data transfers at any moment, hampering businesses abruptly.[66] To meet any new requirements, companies would be required to update their contracts, data-sharing agreements, and data transfer procedures with overseas partners. This may result in higher operating and legal expenses, especially for companies that depend significantly on cross-border data exchanges.[67]

---

[61] Varun Kumar and Ishika Mittal, 'The Digital Personal Data Protection Act, 2023: Overview of the Impact on Data Fiduciaries and the Obligations Placed' (*SCC Times*, 11 March 2024) <https://www.scconline.com/blog/post/2024/03/11/the-digital-personal-data-protection-act-2023-overview-of-the-impact-on-data-fiduciaries-and-the-obligations-placed/> accessed 9 February 2025.

[62] Raghvendra Verma, 'BPO and Cross-Border Data Transfer: A Data Privacy Concern - ET Legalworld' (*ETLegalWorld.com*, 25 June 2024) <https://legal.economictimes.indiatimes.com/news/opinions/bpo-and-cross-border-data-transfer-a-data-privacy-concern/111252382> accessed 9 February 2025.

[63] Regulation (EU) 2016/679 (General Data Protection Regulation) art 46.

[64] 'Cross-Border Data Transfer Under India's DPDP Act' (*Leegality Blog*, December 2023) https://www.leegality.com/consent-blog/cross-border-data-transfer accessed 4 February 2025.

[65] Digital Personal Data Protection Act 2023, s 16(1).

[66] Digital Personal Data Protection Act 2023, s 16(2).

[67] Nydia MacGregor and Tammy L. Madsen, 'Regulatory Shocks: Forms, Dynamics, and Consequences' (*Oxford Research Encyclopedia of Business and Management*, 24 October 2018). <https://oxfordre.com/business/display/10.1093/acrefore/9780190224851.001.0001/acrefore-9780190224851-e-140?p=emailA8hW%2FYY17B5e.&d=%2F10.1093%2Facrefore%2F9780190224851.001.0001%2Facrefore-9780190224851-e-140> accessed 10 February 2025.

The GDPR provides companies with clear routes for compliance by emphasizing on Standard Contractual Clauses and adequacy determiners. A less stable environment is produced by the DPDP Act's reliance on government notifications and the authority to impose limitations at any moment, which may impede global cooperation and data exchange. The DPDP Act in the pretext of 'digital sovereignty', makes it difficult for Data Fiduciaries to comply with its rules on cross-border transfer of data and increases operational costs for them.[68] Furthermore, letting varying international affairs affect fiduciaries would only make it difficult for them to operate in the country, especially international organizations that act as data fiduciaries. This unpredictability can lead to a breach of fiduciary duty by forcing companies to prioritize government-imposed restrictions over their obligation to protect data principals' interests.

LEGAL AND JUDICIAL IMPLICATIONS OF FIDUCIARY DUTIES

The shareholder theory recognises a director's duty to maximise profits, essentially the goals of the shareholder and the firm. Whereas, a stakeholder theory widens the approach by adding the additional burden to the directors to enhance their activities by aligning them with the goals of all stakeholders, including creditors, employees, consumers and even society. [69] It is imperative to analyse the compatibility of DPDP Act with the mandate of fiduciary duties prevalent in the legal, the Companies Act, and judicial sphere, judicial precedents, in India.

The Company Law 2013, in lines of the stakeholder theory, has included Section 166(2), instructing the directors to work in the interests of the "members as a whole".[70] Along with the mention of company, shareholders and employees, the section also included "community" which can be interpreted to mean an assemblage of populations that are mutually interdependent.[71] Landmark judgement, Tata Consultancy Services Limited v. Cyrus Investments Pvt. Ltd. *and* Ors., held that "Section 166(2) is a combination of private interest and public interest",[72] emphasising on the directors' responsibility towards all stakeholders.

[68] Prakhar Tiwari, 'Misuse of Personal Data by Social Media Giants' (2023) 3 Jus Corpus Law Journal 1059.
[69] B. J. McKenna, *Good business; exercising effective and ethical leadershipgood business; exercising effective and ethical leadership, o'toolejames and Mayerdon (eds). New York, NY: Routledge, 2010. 218 pages, paper back.*, 10 ACADEMY OF MANAGEMENT LEARNING & EDUCATION 738–739 (2011).
[70] The Companies Act 2013, s 166(2).
[71] Sagnik Sarkar, 'An Analysis of the Directors' Fiduciary Duty of Loyalty towards Policyholders of Indian Insurance Companies' [2022] SSRN Electronic Journal.
[72] *Tata Consultancy Services Ltd v Cyrus Investments Pvt Ltd and Ors* (2021) AIRONLINE 179 (SC).

The overview of DPDP Act indicates that it is line with broadening the integrity and transparency of the directors, which was held to be fundamental to ethical corporate governance in Satyam Computer Services Ltd. v. Union of India.[73] As observed, there are certain gaps in the Act that do not account for complete transparency, allowing the level of compliance to the firms' discretion. However, the holding in cases such as Piedmont Trading Pvt. Ltd. v. Indian Farmers Fertilizer Cooperative Ltd., which emphasis on the importance of acting in the best interest of the stakeholders,[74] indicate that the companies are not to exploit the loopholes but rather function with the aim of the DPDP Act.

The recognition and implementation of these fiduciary duties in India are a recent development, making it hard to gauge its protentional implementation to the Data Privacy regulations. DPDP Act, being passed in 2023, further lacks precedents to understand the court's view on the laws that appear ambiguous. It is imperative that the courts continue their ongoing trend of holding the firm accountable for its actions that affect the community. This also lays emphasis on the development of stringent legislatures so that the judiciary can use it as a foundation to establish liability on the companies for with respect to their fiduciary duties.

CONCLUSION AND WAY FORWARD

The Digital Personal Data Protection Act 2023 represents an crucial step in building a regulatory regime in India to safeguard personal data. It is undoubtedly a critical development, however, this act suffers from various shortcomings, which can be derived from analysing the need of the hour as well through a comparison with the robust provisions of the GDPR. These potentially hinder the DPDP's objective to protect consumers and establish rules regarding fiduciary duties of agents while handling data, the limitations include: a lack of transparency; inadequate redressal mechanisms for the data principals; incomplete protection for different forms of data; concerns regarding protection over-intervention from government; and compliances for handling children's data. These loopholes aggravate agency problems in that data fiduciaries may end up acting primarily in their interests, foregoing the interest of individuals whose data is being collected and processed.

The shortcomings of the data protection regulations in India, must be dealt in a multi-faceted manner. Indian laws can adopt GDPR regulations in situations where it finds DPDP Act

[73] *Satyam Computer Services Ltd v Union of India* (2011) 7 SCC 791 (SC).
[74] *Piedmont Trading Pvt Ltd v Indian Farmers Fertilizer Cooperative Ltd* (2014) 3 SCC 381 (SC).

lacking. Since multinational corporations are already complying to these norms, it will also ease the regulatory frameworks internally, speeding up the process. The Records of Processing Activities, which is mandate under the GDPR can be adopted to include information that are presently lacking in transparency.[75] Another important step to protect the data principals is through increasing awareness relating to data privacy, consequently improving the value of informed consent.[76] Alongside, compensation to individuals should be introduced to increase trust and confidence in the users. With the increasing AI usage, safeguards regarding data in this also requires development, to keep up with the changing digital era.[77]

The agency problem is not mitigated entirely though the DPDP Act, but with the combination of the Companies Act regulations and judicial intervention, it can be developed into a more comprehensive regulation. Nonetheless, this is a rather slow process, with several debates which is unlikely to keep up with the ongoing rapid digitalisation. An amendment to the Act or further guidelines released on application of the Act are effective for the optimal protection of data of all parties concerned, eliminating the possibility of firms' interest dominating over its stakeholders. A proactive and adaptive regulatory framework that prioritizes both individual rights and corporate accountability will be essential to navigate the complexities of the digital landscape and ensure that the interests of all stakeholders are protected.

[75] Regulation (EU) 2016/679 (General Data Protection Regulation) art 30.
[76] Ponnurangam Kumaraguru and Lorrie Cranor, 'Privacy in India: Attitudes and Awareness' (2005) 3856 Lecture Notes in Computer Science 243.
[77] Paarth Naithani, 'Regulating artificial intelligence under data protection law: Challenges and solutions for India' (2023) 14 Indian JL & Just 436.