OBSERVER RESEARCH FOUNDATION

The Dialogue®
INFORM ENGAGE IDEATE

PRIVACY IN PRACTICE
STRATEGIES FOR DATA MANAGEMENT IN INDIA

KAZIM RIZVI and SHRAVISHTHA AJAYKUMAR
Editors

PRIVACY IN PRACTICE

STRATEGIES FOR DATA MANAGEMENT IN INDIA

Attribution: Kazim Rizvi and Shravishtha Ajaykumar, Eds., *Privacy in Practice: Strategies for Data Management in India*, January 2025, Observer Research Foundation.

ISBN: 978-81-19656-82-0
ISBN Digital: 978-81-19656-94-3

All images used in this report are from Getty Images: p9 - anand purohit; p40 - deepart386; pp63 & 88 - SOPA Images; pp118 & 146 - Andriy Unofriyenko.

Editorial and Production Team: Vinia Mukherjee, *Editor and Producer;* Akriti Jayant, *Editor, The Dialogue;* Aswathy Gopinath and Monika Ahlawat, *Assistant Editors;* Rahil Miya Shaikh, *Design and Layout*

Contents

INTRODUCTION

Kazim Rizvi and Shravishtha Ajaykumar

The Digital Personal Data Protection (DPDP) Act, enacted in 2023, is essential to India's aim of providing its people an environment that protects privacy. The DPDP Act has established data protection and privacy standards for India and established regulatory clarity. This legislation sets obligations for data fiduciaries and significant data fiduciaries, provides safeguards for children's data, vests rights in individuals, allows cross-border data transfers, and provides a contour for a data protection board, financial penalties, and a grievance management system.

While the DPDP Act's framework of data protection and compliance is agnostic both, vertically (across maturity levels of businesses) and horizontally (across different sectors), the implementation approach will likely differ for various stakeholders.

For example, in emerging economies like India, start-ups and small-scale enterprises are still in the process of understanding compliance with data protection norms, whereas larger organisations that have aligned to existing international norms face less pressure.

To be sure, the DPDP Act 2023 is not India's first attempt to regulate personal data. Various sector-specific regulations exist, and directly or indirectly apply to managing personal data in India, which may result in differences in how compliance is operationalised for specific sectors. Therefore, from an industry perspective, it would be beneficial to provide more precise direction to businesses about key data protection and privacy concepts and how compliance requirements and architectures may change with the implementation of the DPDP Act. In this context, this compendium examines what is next in data protection by mapping operationalisation strategies for the new data protection regime.

The compendium explores the issues related to data protection and management in India with respect to six representative sectors and domains: financial, health, education, cloud services, biometrics, and emerging technologies. The section on financial services caters to fintech service providers that use digital technologies for fraud detection, algorithmic trading, credit lending, and robo-advisory. The healthcare chapter, meanwhile, discusses the use case of the DPDP Act in the digital health sector, including in activities such as healthcare analysis, precision medicine, and predictive diagnosis. The articles on education data, for their part, discuss the compliance constraints faced by edtech platforms that deliver educational services online, particularly the age-verification mandate.

The fourth section, on data processors, explores both the direct and indirect implications of the DPDP Act for data processors and the impact they could have on cloud service-based security and ensuring infrastructural reliability. The essays on biometric data follow, discussing the foundational nature of biometric data use in India, the principles of biometric data management, and how individuals can be better protected when submitting their biometric data. Lastly, the sixth section discusses the impact of the DPDP Act on emerging technologies, highlighting the importance of Artificial Intelligence (AI), as a large language model, its reliance on data and the need for anonymisation.

The essays in this compendium delve into the details of sectoral data-protection compliance. One step further, they also bring out the equally relevant vertical aspects by understanding how the maturity levels of businesses within that sector need to be considered while laying down the roadmap for data compliance.
While the functions and targets of data-driven companies are determined by their specific business models and requirements, they follow broadly similar steps when dealing with data to extract value. Keeping this in mind, this

compendium suggests a unique data lifecycle-based framework to map the compliance roadmap for businesses. The framework divides the data lifecycle into six stages—i.e., data collection, data retention, data structuring, data transfer, data processing, and data expunction. Adopting this framework will allow data fiduciaries clarity on the provisions to be incorporated at various data lifecycle stages. This volume discusses the nuances of such provisions by mapping the processes involved, the timelines, compliance requirements, and impact at the vertical level. Moreover, it discusses how to operationalise these provisions using tech solutions.

The compendium is an exercise in gathering expert and academic opinions in the aforementioned sectors. The aim is to inform smaller, independent organisations centred in India of the ways they can adapt to the DPDP Act 2023 as well as the data privacy rules currently underway.

Kazim Rizvi is Founding Director, The Dialogue.

Shravishtha Ajaykumar is Associate Fellow, Centre for Security, Strategy and Technology, Observer Research Foundation.

01

BIOMETRIC DATA

Academic Perspective

Paarth Naithani and Indranath Gupta

An Application Perspective

Isha Suri and Pallavi Bedi

Key Takeaways

Basu Chandola

Academic Perspective

Paarth Naithani and Indranath Gupta

Biometric data encompasses various identifiers, including facial images, fingerprints, iris scans, and other personal data derived from the measurement or technical processing of physical, physiological, or behavioural characteristics.[1] These identifiers allow for the unique identification of individuals, making biometric data a distinctive form of personal information. The attributes of this data are such that individuals can be accurately identified. Further, these identifiers are indelible; once assigned, they cannot be changed or disassociated.[2] Consequently, the privacy risks associated with biometric data are significantly heightened. This type of data is inherently sensitive, often collected through contactless and ubiquitous technologies, and has unprecedented potential for use in surveillance activities.[3] Moreover, biometric data is non-revocable—i.e., any misappropriation or misuse of

this information entails substantial risks for individuals.[4]

In this context, this article examines the Digital Personal Data Protection Act (DPDP), 2023, assessing the advantages and disadvantages of the absence of a separate protection category for sensitive personal data. It explores the nature of protection accorded to biometric data in various jurisdictions and suggests pathways for India's own regulatory framework. This article also considers international approaches to regulating biometric data and highlights key considerations for future regulatory frameworks.

The Legislative History of Protecting Biometric Data Leading Up to DPDP

The DPDP Act 2023 replaces Section 43A of the IT Act. Under Section 43A of the Information Technology Act (IT Act), there exists a provision for regulating biometric data in India. This section holds corporate entities accountable for failing to protect personal data. The relevant conditions apply when a corporate body that possesses, manages, or handles sensitive personal data or information in a computer resource is negligent in maintaining reasonable security practices, thereby causing wrongful loss or gain to any person.[5] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, enacted under Section 43A, defined 'sensitive personal data' to include biometric data.

The legislative history leading to the enactment of the DPDP Act 2023 includes references to biometric data through the Personal Data Protection Bill, 2018 (PDP, 2018) and the Personal Data Protection Bill, 2019 (PDP, 2019).[6]

The PDP, 2018 explicitly defined biometric data and classified it as "sensitive" personal data.[7] It mandated that data fiduciaries processing biometric data conduct prior data-protection impact assessment.[8] Additionally, it prohibited the processing of certain forms of biometric data as notified by the Union government.[9] The PDP, 2018 also established explicit consent as a norm for processing sensitive personal data,[10] defining "explicit consent" as fulfilling the requirements of ordinary consent. Clause 12 requires that ordinary consent be free, informed, specific, clear, and capable of being withdrawn. It also specifies that consent must be "(a) informed, having regard to whether the attention of the data principal has been drawn to purposes for operations in processing that may have significant consequences for the data principal; (b) clear, having regard to whether it is meaningful without recourse to inference from conduct in a context; and (c) specific, having regard to whether the data principal is given the choice of separately consenting to the purposes of, operations in, and the use of different categories of sensitive personal data relevant to processing."[11]

Additionally, sensitive personal data may be processed if strictly necessary for certain functions of the State,[12] in

compliance with law or any order of any court or tribunal,[13] or where processing is strictly necessary to take prompt action, such as a medical emergency.[14] The PDP, 2018 also recognised that "[a]ny person who alone or jointly with others, knowingly or intentionally or recklessly, in contravention of the provisions of this Act" obtains, discloses, transfers, sells, or offers to sell sensitive personal data which results in harm to the data principal shall be punishable with five years of imprisonment.[15] It recognised that the Data Protection Authority (DPA) can issue Codes of Practice concerning the processing of sensitive personal data.[16] Further, a penalty extending to four percent of worldwide turnover for processing sensitive personal data in violation of the Act's provisions was proposed.[17]

Similarly, the PDP, 2019 defined biometric data[18] and reaffirmed its classification as sensitive personal data.[19] It retained the requirements for conducting data-protection impact assessments and barred the processing of specific types of sensitive personal data[20] as notified by the Central Government.[21] Explicit consent remained a cornerstone for processing sensitive personal data.[22] However, the PDP, 2019 also allowed for the processing of personal data necessary for employment-related purposes, such as attendance verification, with specific limitations on sensitive personal data.[23] It mandated that copies of sensitive personal data be stored in India even if they are transferred outside the country[24] and stipulated that such transfers could occur only with the explicit consent of the Data Principal.[25] Additionally, it acknowledged the potential formulation of Codes of Practice for processing sensitive personal data.[26]

Unlike these draft proposals, the DPDP Act 2023 does not categorise biometric data as sensitive personal data,[27] nor does it recognise sensitive personal data as a distinct category. A preliminary reading suggests that personal data encompasses sensitive personal data, with all types of data being treated equally. While this approach may create stability and uniformity for data fiduciaries, it lacks a specific operational framework addressing the heightened privacy risks associated with more sensitive data types. The horizontal protection of all data may not adequately safeguard the interests of data principals, given the reduced thresholds in place.

Compared to previous drafts, the DPDP Act represents a shift regarding the protection of sensitive personal data, including biometric data.

Regulation of Biometric Data in the EU and Other Jurisdictions

In the European Union (EU), biometric data is classified as a distinct category of personal data.[28] The General Data Protection Regulation (GDPR) imposes a general prohibition on processing biometric data without explicit consent or other legal grounds.[29] "Explicit consent", as defined by the GDPR,[30] necessitates a higher threshold than "general consent"

and requires additional verification to ensure that data subjects have provided informed consent.[31]

Additionally, in the EU, "the purpose for which consent is given must be necessary […] Necessity […] does not demand that data processing is the only way to achieve the given aim, but it does require that the goal cannot be achieved by other, less intrusive means (proportionality between the intrusion involved in the data processing and that aim)."[32] This stipulation indicates that processing personal data is not an obvious choice; it becomes an option only when alternative measures cannot fulfil the objective.

Article 22 of the GDPR provides specific rights against automated decision-making when such decisions affect data subjects.[33] While explicit consent can be a ground for automated processing,[34] this provision has been scrutinised in the context of facial recognition technologies. For instance, in France, the use of automated facial recognition for monitoring school attendance was deemed invalid due to concerns that the consent obtained from high school students was not given freely, specifically, or informedly. Additionally, it was determined that schools could employ less intrusive methods, such as badge checks and CCTV, to control students' access.[35] Here, the principle of proportionality was pivotal, reinforcing that sensitive personal data should not be processed if other available options suffice.

In another instance, the power imbalance between schools and students was found to render students' consent invalid, as the latter could not exercise free will in agreeing to the processing of their biometric data.[36] This scenario is akin to standard agreements lacking negotiation scope, where one party cannot freely choose, and consequently, consent loses its validity.[37]

A Bulgarian Data Protection Authority (DPA) opinion also invalidated the use of automated facial recognition for student access control. It stated that such measures failed to comply with Article 22 of the GDPR and should avoid processing special categories of data.[38]

The data protection principles enshrined in the GDPR, including data minimisation and storage limitation, apply equally to biometric data. The Information Commissioner's Office (ICO) in the UK recommends limiting the use of biometric data to the minimum that is "adequate, relevant and necessary for [the] purpose."[39] According to the ICO, data controllers "must consider storage limitation throughout the lifecycle of personal information as it passes through a biometric recognition system. [The data controller] must have processes in place to regularly review [their] database of biometric references to ensure [they] delete any data that [they] no longer need. [They] must have clear retention periods, which means [they] only keep this information in an identifiable form for as long as is necessary."[40] The ICO guidelines emphasise the need to forgo

storage in perpetuity, with the purpose determining the duration of storage. Therefore, data controllers should avoid unnecessary storage, as it contravenes data protection principles.

Another crucial principle that is applicable to biometric data is data protection by design. By employing pseudonymisation and various technical and organisational measures, data controllers can enhance data minimisation and safeguard data subjects' interests.[41]

The EU also recognises the necessity and proportionality principle concerning measures that infringe biometric data privacy. In *S. and Marper v. The United Kingdom,*[42] the European Court of Human Rights determined that the indiscriminate retention of fingerprints and DNA profiles from individuals who are not convicted of crimes constituted a disproportionate interference with the right to respect for private life, lacking a necessary purpose within a democratic society.[43]

Recent developments, such as the EU's Artificial Intelligence Act (2024), impose a ban on the use of AI systems for real-time remote biometric identification of individuals in public spaces for law enforcement,[44] reflecting concerns over intrusive surveillance and its implications for fundamental rights.[45] The AI Act categorises "biometric identification and categorisation of natural persons" as high-risk AI,[46] subjecting it to stringent requirements. The use of high-risk AI systems comes with various requirements. The AI Act mandates the establishment and implementation of a risk-management system for these systems.[47] Furthermore, developers must create high-risk AI systems using training, validating, and testing datasets that meet quality criteria.[48] Before these systems enter the market, they must prepare technical documentation.[49] Additionally, developers must ensure that the high-risk AI systems that they design and develop are equipped to maintain logs during operation.[50] Moreover, natural persons must effectively oversee high-risk AI systems throughout their usage.[51] Finally, developers must ensure that high-risk AI systems achieve "an appropriate level of accuracy, robustness, and cybersecurity, and perform consistently in those respects throughout their lifecycle."[52] The AI Act emphasises the need for transparency in operations, enabling users to interpret systems' outputs.[53]

Notable features of data protection laws in other jurisdictions are worth highlighting. For example, Canada employs a flexible approach to sensitive personal data categorisation, lacking a predetermined list of such data.[54] In Canada, "any personal information can be sensitive depending on the context"[55] and emphasises the necessity of express consent for processing biometric data, stating, "[w]here biometric technology is used for non-integral or non-essential collections, uses, or disclosures, you must provide individuals with other means of access or participation."[56] Canada further asserts that one "must not analyse biometric data to extract such additional information not originally consented to, and even then, only if appropriate."[57]

In Australia, biometric data qualifies as sensitive personal data, and entities cannot collect sensitive information without express consent. For an agency, the information must be "reasonably necessary for, or directly related to, one or more of the entity's functions or activities"; for an organisation, it must be "reasonably necessary for one or more of the entity's functions or activities."[58]

South Africa prohibits the processing of sensitive personal data, although this prohibition does not apply if the data subject has consented or under other specific grounds.[59]

Grounds for Processing Biometric Data

The DPDP Act 2023 outlines specific grounds for processing personal data, notably consent and legitimate use. When consent is the basis for processing, it must be free, specific, informed, unconditional, and unambiguous.[60] Given the heightened risks associated with biometric data, it is crucial to interpret these conditions stringently. Ensuring free, informed, and unconditional consent allows the data principal to be fully aware of biometric data-processing activities and to avoid any coercion in sharing their data. Importantly, data principals retain the right to withdraw consent at any time, and this withdrawal should be as straightforward as the initial granting of consent.[61] Upon receiving a withdrawal request, the data fiduciary is obligated to cease processing the personal data within a reasonable timeframe and ensure that its data processors do the same.[62]

Additionally, the DPDP Act mandates that, when seeking consent, data fiduciaries must provide notice to the data principal regarding "the personal data and the purpose for which the same is proposed to be processed."[63] For instance, the DPDP illustrates the following: "X, an individual, opens a bank account using the mobile app or website of Y, a bank. To complete the Know-Your-Customer requirements under law for opening of bank account, X opts for processing of her personal data by Y in a live, video-based customer identification process. Y shall accompany or precede the request for the personal data with notice to X, describing the personal data and the purpose of its processing."[64] This example illustrates the application of the notice and consent framework in India. Sensitive personal data, including biometric data, still requires adequate notice from the data fiduciary prior to processing.

Another basis for processing data is legitimate use when the data principal voluntarily provides data without indicating non-consent.[65] It is essential to interpret this provision strictly and to implement safeguards to prevent the wrongful assumption of voluntariness and the absence of consent when processing biometric data. One legitimate use case is "(i) for the purposes of employment or those related to safeguarding the employer from loss or liability, [..] or provision of any service or benefit sought by a Data Principal who is an employee."[66] There needs to be clarification on whether this ground for legitimate use applies to sensitive and biometric data processing

for employment purposes. Previously, the PDP, 2019, allowed only the processing of personal data (excluding sensitive personal data) for employment purposes.[67]

Since the DPDP Act 2023 lacks specific provisions on sensitive personal data, the accompanying Rules must clarify the regulation of biometric data.

Implementation Recommendations

The rules under the DPDP Act should specify that certain categories of data carry a higher privacy risk than ordinary personal data, necessitating enhanced protection measures. The Srikrishna Committee[68] highlighted the importance of providing a higher level of protection for sensitive personal data, given its close relation to an individual's identity and the potential for significant harm.[69] Stricter regulations are essential to mitigate such risks,[70] including establishing a higher consent threshold for processing sensitive data. Additionally, the Committee emphasised the principles of necessity and proportionality when processing biometric data. For example, law enforcement agencies must demonstrate that the collection of biometric information is necessary and proportional to the investigation at hand.[71]

Defining sensitive personal data is crucial, especially for understanding when personal data becomes sensitive. Answering this question is complex, as advances in computing power and big data have changed the nature of sensitive information. It is important to recognise that "the sensitive nature of a particular dataset may no longer be as intuitively obvious as it has been in the past."[72] Furthermore, data sensitivity "can depend on the legal and sociological context of a country."[73] As such, categorising data as sensitive can hinge on the effects of data processing. A contextual approach to defining sensitive personal data suggests that "any personal data can become sensitive depending on the circumstances and the manner in which it is being processed."[74]

If the Rules do not distinctly categorise sensitive personal data, all data will be treated as personal data, processed based on general consent or legitimate use. In this scenario, the law's provisions with regard to biometric data processing should be strictly applied and interpreted. For example, it is essential to recognise that using biometric data for purposes other than those for which it was collected undermines informational autonomy.[75] Moreover, the DPDP provides exemptions on various grounds, including crime prevention, investigation, and prosecution.[76] It is vital to acknowledge that these exemptions are subject to the principles of necessity and proportionality. Additionally, consent—not legitimate use—should serve as the basis for biometric data processing, with individuals retaining the right to refuse non-essential processing.

Considering whether sensitive personal data categorisation is necessary for adequate protection raises interesting points. One perspective emphasises that

categorising sensitive personal data is essential because certain types of data pertain to "intimate matters in which there is a higher expectation of privacy. Unauthorised use of such information of the individual may have severe consequences."[77] This unauthorised use can lead to discriminatory actions against individuals and "is more likely to lead to discrimination, ridicule and reputational harm, especially where one's beliefs and choices form part of the minority view in society. This in turn would cause greater harm to the person in the form of loss of dignity and personhood. […] [It] could result in the stereotyping and pre-judging of persons, which may affect their ability to fully develop their personality."[78] The potential for high intrusion when sensitive data is processed without authorisation[79] underscores the need for categorisation and explicit consent to mitigate the risk of misuse.[80] In routine, low-risk transactions, general consent can suffice instead of explicit consent.[81]

Conversely, some argue that since the DPDP Act 2023 does not distinguish between sensitive personal data and ordinary personal data, all data should be treated equally in terms of the consent requirement. Under the DPDP Act 2023, the consent requirement can safeguard all data if the conditions are strictly enforced. For instance, enforcing free, informed, and unconditional consent ensures that no data is collected without notifying the data principal and allowing them to make genuine choices about consent, without it being mandatory to proceed. Therefore, the absence of sensitive data categorisation is not a matter of concern if a high consent threshold is maintained across all circumstances, enabling individuals to make informed decisions and avoid potential harm.

The Way Forward

Biometric data is highly sensitive personal information that presents privacy risks. Notably, the DPDP Act does not consider biometric or sensitive personal data as a distinct category. Insights from the EU and other jurisdictions that recognise biometric data as sensitive, necessitating explicit consent rather than ordinary consent, can be used to guide regulation.

At the same time, further research is needed to assess the benefits and impacts of maintaining two separate categories of consent. Does this distinction provide greater clarity to data controllers and effectively safeguard the rights of data subjects? A number of EU judgments underscore the significance of free and unconditional consent when utilising biometric data, particularly given the power imbalance between data subjects and controllers. Furthermore, the EU emphasises the necessity and proportionality of measures that infringe on biometric data privacy. The recent EU AI Act classifies AI systems using biometric data as high-risk and prohibits their use for "real-time" remote biometric identification in public for law enforcement purposes. This legislation outlines various requirements for classifying biometric data as high-risk AI, which the DPDP Act 2023 Rules could adapt for the Indian

context. However, the advantages of a two-layered consent approach must be carefully weighed against a strategy that implements a single, higher consent threshold.

The DPDP Act 2023 Rules should clarify whether biometric data qualifies as sensitive personal data necessitating enhanced protection. In light of technological advancements and big data analytics, establishing a definition for sensitive personal data is essential. Several alternatives for regulating sensitive personal data exist, including the following:

- Prohibiting the processing of sensitive personal data, except under narrow exceptions
- Allowing the processing of sensitive personal data only under narrower grounds than those applicable to all personal data
- Not prescribing general safeguards, but permitting the incorporation of such safeguards based on the context of collection, use, disclosure, and potential harms
- Not mandating specific safeguards but allowing for more stringent penalties in cases of harm resulting from the processing of sensitive personal information[82]

Conversely, if the Rules do not classify sensitive personal data as a separate category, the existing provisions of the DPDP Act 2023 must be strictly interpreted. The necessity of free and unconditional consent should be acknowledged, and using biometric data for purposes other than those specified at the time of collection must be restricted. Additionally, the principles of necessity and proportionality should guide the processing of biometric data. Similar to regulations in other jurisdictions, processing should not be the default choice to achieve a particular objective; instead, less intrusive alternatives should be explored. This foundational norm can extend to various forms of processing, including that of sensitive and biometric data.

Indranath Gupta is Professor, Jindal Global Law School, O.P. Jindal Global University, Sonipat, India.

Paarth Naithani is Lecturer, Jindal Global Law School, O.P. Jindal Global University, Sonipat, India.

Endnotes

1 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill, Clause 3(8)*, 2018, https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

2 CNIL, *Facial Recognition For a Debate Living Up To The Challenges,* National Commission on Informatics and Liberty, https://www.cnil.fr/sites/cnil/files/atoms/files/facial-recognition.pdf.

3 "Facial Recognition For a debate living up to the challenges"

4 "Facial Recognition For a debate living up to the challenges"

5 Section 43A: Compensation for Failure to Protect Data, Information Technology Act

6 India Code, *Rule 3, The Information Technology (Reasonable Security, Practices, and Procedure and Sensitive Personal Data or Information) Rules,* 2011

7 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 3(35)*, 2018

8 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 33,* 2018

9 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 106,* 2018

10 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 18,* 2018

11 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 18,* 2018

12 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 19,* 2018

13 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 20,* 2018

14 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 21,* 2018

15 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 91,* 2018

16 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 61,* 2018

17 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 69,* 2018

18 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 3(7),* 2019

19 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 3(36),* 2019

20 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 27,* 2019

21 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 92,* 2019

22 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 11,* 2019

[23] Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 13,* 2019

[24] *Ministry of Electronics and Information Technology, The Personal Data Protection Bill Clause 33,* 2019

[25] Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 34,* 2019

[26] Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 50,* 2019

[27] Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act," 2023

[28] General Data Protection Regulation, "Article 4(14)- Definitions," https://gdpr-info.eu/art-4-gdpr/

[29] General Data Protection Regulation, "Article 9: Processing of Special Categories of Personal Data," https://gdpr-info.eu/art-9-gdpr/

[30] General Data Protection Regulation, "Article 9: Processing of Special Categories of Personal Data," https://gdpr-info.eu/art-9-gdpr/

[31] ICO, "What Are the Conditions For Processing?," https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-are-the-conditions-for-processing/

[32] Vera Lúcia Raposo, "(Do Not) Remember My Face: Uses of Facial Recognition Technology in Light Of The General Data Protection Regulation," *Information & Communications Technology Law* 32, no. 1 (2023).

[33] General Data Protection Regulation, "Article 22- Automated Individual Decision-making, including profiling," https://gdpr-info.eu/art-22-gdpr/

[34] General Data Protection Regulation, "Article 22- Automated Individual Decision-making, including profiling," https://gdpr-info.eu/art-22-gdpr/

[35] Sebastião Barros Vale and Gabriela Zanfir-Fortuna, "Automated Decision-Making Under the GDPR: Practical Cases From Courts and Data Protection Authorities," Future of Privacy Forum, https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf.

[36] "Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities"

[37] "Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities"

[38] "Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities."

[39] ICO, "How Do We Keep Biometric Data Secure?," https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/.

[40] "How Do We Keep Biometric Data Secure?"

[41] General Data Protection Regulation, "Article 25- Data Protection by Design and by Default," https://gdpr-info.eu/art-25-gdpr/

[42] Case of S. and Marper v. The United Kingdom, European Court of Human Rights, 4 December 2008, Applications nos. 30562/04 and 30566/04

[43] Case of S. and Marper v. The United Kingdom, European Court of Human Rights, Applications nos. 30562/04 and 30566/04, https://rm.coe.int/168067d216.

[44] EU Artificial Intelligence Act, "Recital 18," https://artificialintelligenceact.eu/recital/18/

[45] "Recital 18"

[46] EU Artificial Intelligence Act, "Annex III-High-Risk AI Systems Referred to in Article 6(2)," https://artificialintelligenceact.eu/annex/3/

[47] EU Artificial Intelligence Act, "Article 9- Information to be Submitted upon the Registration of High-Risk AI Systems Listed in Annex III in Relation to Testing in Real World Conditions in Accordance with Article 60," https://artificialintelligenceact.eu/annex/9/

[48] EU Artificial Intelligence Act, "Article 10- Union Legislative Acts on Large-Scale IT Systems in the Area of Freedom, Security and Justice," https://artificialintelligenceact.eu/annex/10/

[49] EU Artificial Intelligence Act, "Article 11-Technical Documentation Referred to in Article 53(1), Point (a) – Technical Documentation for Providers of General-Purpose AI Models," https://artificialintelligenceact.eu/annex/11/#:~:text=This%20Annex%20specifies%20what%20documentation,data%20used%2C%20and%20energy%20consumption.

[50] EU Artificial Intelligence Act, "Article 12- Transparency Information Referred to in Article 53(1), Point (b) – Technical Documentation for Providers of General-Purpose AI Models to Downstream Providers that Integrate the Model into Their AI System," https://artificialintelligenceact.eu/annex/12/

[51] EU Artificial Intelligence Act, "Article 14-Human Oversight," https://artificialintelligenceact.eu/article/14/

[52] EU Artificial Intelligence Act, "Article 15-Accuracy, Robustness and Cybersecurity," https://artificialintelligenceact.eu/article/15/

[53] EU Artificial Intelligence Act, "Article 13- Criteria for the Designation of General-Purpose AI models with Systemic Risk Referred to in Article 51," https://artificialintelligenceact.eu/annex/13/

[54] Committee of Experts on a Data Protection Framework, "White Paper of the Committee Of Experts on a Data Protection Framework For India," https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf)

[55] Office of the Privacy Commissioner of Canada, "OPC Updates Guidance Regarding Sensitive Information," https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_210813/

[56] Office of the Privacy Commissioner of Canada, "Draft Guidance for Processing Biometrics – For Organizations," https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-bio/gd_bio_org/

[57] "Draft Guidance for Processing Biometrics – For Organizations."

[58] Office of Australian Information Commissioner, "Read the Australian Privacy Principles," https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles

[59] Sections 26-27, Protection of Personal Information Act (POPI Act) https://popia.co.za

[60] Ministry of Electronics and Information Technology, "Section 6-Digital Personal Data Protection Act," 2023

[61] Ministry of Electronics and Information Technology, "Section 6(4)-Digital Personal Data Protection Act," 2023

[62] Ministry of Electronics and Information Technology, "Section 6(6) Digital Personal Data Protection Act," 2023

[63] Ministry of Electronics and Information Technology, "Section 5 Digital Personal Data Protection Act," 2023

[64] Ministry of Electronics and Information Technology, "Section 5 Digital Personal Data Protection Act," 2023

65 Ministry of Electronics and Information Technology, "Section 7(a) Digital Personal Data Protection Act," 2023

66 Ministry of Electronics and Information Technology, "Section 7(i) Digital Personal Data Protection Act," 2023

67 Ministry of Electronics and Information Technology, *The Personal Data Protection Bill Clause 13*, 2019

68 "White Paper of the Committee of Experts on a Data Protection Framework for India"

69 B.N. Srikrishna et al., "White Paper of the Committee of Experts On a Data Protection Framework For India," Ministry of Electronics and Information Technology, https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf

70 "White Paper of the Committee of Experts On a Data Protection Framework For India."

71 "White Paper of the Committee of Experts On a Data Protection Framework For India."

72 Paul Quinn and Gianclaudio Malgieri, "The Difficulty Of Defining Sensitive Data—The Concept Of Sensitive Data In the EU Data Protection Framework," *German Law Journal* 22, no. 8 (2021).

73 Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act, 31*, 2023

74 Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act, 30*, 2023

75 NITI Aayog, "Responsible AI For All: Adopting the Framework – A Use Case Approach On Facial Recognition Technology," https://www.niti.gov.in/sites/default/files/2022-11/Ai_for_All_2022_02112022_0.pdf?trk=public_post_comment-text

76 Section 17(1)(c), DPDP, 2023

77 "White Paper Of the Committee Of Experts On a Data Protection Framework For India,"

78 "White Paper Of the Committee Of Experts On a Data Protection Framework For India."

79 "White Paper Of the Committee Of Experts On a Data Protection Framework For India."

80 "White Paper Of the Committee Of Experts On a Data Protection Framework For India."

81 "White Paper Of the Committee Of Experts On a Data Protection Framework For India."

82 "White Paper Of the Committee Of Experts On a Data Protection Framework For India."

An Application Perspective

Isha Suri and Pallavi Bedi

The use of biometric systems has been on the rise in India across both private and government sectors. Globally, the demand for biometric recognition is expected to grow significantly, with market revenues projected to almost double from US$43 billion in 2022 to US83 billion by 2027.[1] Biometric systems are increasingly viewed as replacements for conventional identification and verification methods such as physical checks, photo IDs, tokens, and passwords, offering enhanced security and convenience in various applications.[2]

The Digital Personal Data Protection (DPDP) 2023 does not specifically define 'biometric data'. Reference may be drawn, however, from Section 2(b) of The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which

defines 'biometrics' as "technologies that measure and analyse human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements, and DNA for authentication purposes."[3] The physical and behavioural features recorded by a biometric system—such as a person's face, fingerprints, or voice—are referred to as "biometric characteristics".[4]

Many biometric characteristics, such as fingerprints, irises, and DNA, are highly unique, with minimal overlap between individuals. This uniqueness is also recognised by laws such as the Illinois Biometric Information Privacy Act (BIPA), which emphasises that "biometrics are unlike other unique identifiers used to access finances or other sensitive information." Once breached, the individual faces a heightened risk of identity theft and may withdraw from biometric-enabled transactions entirely. Thus, the risks associated with biometric data breaches are far greater than those associated with non-biometric data. Other than the fact that a person cannot change their biometric characteristics, such data can also reveal highly intimate and sensitive information. Ensuring robust protection measures for biometric data is paramount.

Recent incidents highlight the critical vulnerabilities associated with biometric data. Between 2021 and 2024, in India, the personal information of thousands of law enforcement officials and individuals applying to be police officers was leaked online, exposing highly sensitive biometric information, including fingerprints, facial scan images, signatures, and details of tattoos and scars on their bodies.[5] Around the same time, cybercriminals began advertising the sale of similar biometric police data from India on platforms such as the messaging app Telegram.[6] These breaches are especially alarming as they increase the risk of identity theft and enable more sophisticated fraud. Criminals have already posed as law enforcement agencies in cases of cyber fraud, leading to wrongful digital arrests.[7] These incidents highlight the compelling need for stronger protections to safeguard biometric data.

The need for protection mechanisms becomes more urgent as Closed Circuit Television (CCTV) cameras, for example, are now ubiquitous, permeating across spaces like public buildings and streets, and shopping and recreation areas. While facial recognition technology remains primarily limited to certain government agencies and large private entities, CCTV cameras have become a common household purchase due to advancements that have lowered their cost. In India, the increasing number of CCTV cameras is often viewed as a sign of progress and an effort to create safer cities. The country is also a witnessing the enthusiastic adoption of CCTV cameras for surveillance among private actors; employers use them to track worker attendance, and private residential areas install them to enhance security. This practice is also being incentivised by some state governments. For example, as early as 2014, under the Gujarat government's Suraksha Setu Project, building societies

were reimbursed for 30 percent of the total cost of CCTV installation,[8] with the state's police departments managing the initiative. In 2019, the Delhi government introduced subsidies on the electricity consumed by CCTV cameras that faced outwards from homes.[9]

The following points outline the privacy concerns associated with the use of biometric data:

- **Covert collection:** Facial features can be captured through widespread CCTV use without prior knowledge or consent, violating the principle of informed consent. Similarly, new iris-based systems can surreptitiously capture images of a person's eyes from up to two metres away without their permission.
- **Cross-matching:** Using biometric data beyond its original purpose breaches the principle of 'purpose limitation'[a] This cross-use of data can have significant privacy implications.
- **Secondary information:** Biometric data is often a unique identifier and can reveal secondary personal information unrelated to its original collection purpose. For example, iris images or DNA can divulge sensitive and intimate information about a person's health, while fingerprints may offer insights into an individual's occupation or socio-economic status.[10]

The Current Regulatory Landscape in India

The use of biometric data is governed under the DPDP Act, 2023. However, the DPDP Act does not classify biometric data as sensitive personal information, unlike regulatory practices in other jurisdictions. Thus, while biometric data is covered under the DPDP Act, it is not subject to heightened protections.

Until the DPDP Act is officially enforced, private entities handling biometric data are regulated by Section 43A of the IT Act, which categorises biometric data as sensitive personal information and places specific obligations on those entities.[11] Moreover, during research conducted by these authors, stakeholders highlighted the need to harmonise definitions between the two laws for clearer guidance on processing such data.

Although the state processes vast amounts of biometric data, the DPDP Act grants extensive exemptions for state entities and those functioning as instrumentalities of the state. Notably, it does not apply to government entities. Given the scale of biometric data that is processed by the state, it is crucial to bring these entities within the scope of the DPDP Act. For example, between 2019 and 2023, a number of facial recognition technology (FRT) projects at

[a] Purpose limitation is one of seven core privacy principles. It means that the data is processed and used only for the specified purpose for which consent has been obtained.

the state and city levels were initiated in Odisha, Haryana, Uttar Pradesh, Uttarakhand, Bihar, Delhi, Jammu and Kashmir, Rourkela, Hyderabad, Chennai, Chandigarh, and Dharamsala. The FRT and CCTV projects in Hyderabad were even the focus of Amnesty International's 'Ban the Scan' global campaign against FRT.[12]

Impact of DPDP Act, 2023

The DPDP Act will regulate biometric data as 'personal data', which can only be processed for lawful purposes with the individual's consent. Key aspects of the consent include the following:

- The Data Fiduciary must provide the Data Principal with a notice explaining the details of the personal data being collected and the purpose of processing when requesting consent. Individuals may withdraw their consent at any time. However, consent will not be required for certain "legitimate uses", including: (i) when the individual voluntarily provides data for a specified purpose and has not explicitly declined consent, (ii) when the government is providing a benefit or service, (iii) during a medical emergency, or (iv) for employment purposes. For individuals under 18 years of age, their parent or legal guardian will provide consent.[13]
- Furthermore, the Act imposes the following obligations on Data Fiduciaries (entities responsible for determining the purpose and means of processing):
  (i) Make reasonable efforts to ensure the accuracy and completeness of data
  (ii) Implement robust security safeguards to prevent data breaches
  (iii) Notify the Data Protection Board of India and affected individuals in the event of a breach, and
  (iv) Erase personal data once its purpose has been fulfilled, unless retention is required for legal reasons (storage limitation)

However, for government entities, the storage limitation and the right of the data principal to erasure will not apply.[14]

Qualitative interviews conducted by these authors with select stakeholders revealed that the impact of the DPDP Act will vary based on the size of entities, their geographic scope, and the sector in which they operate. Multinational corporations that are already compliant with frameworks like the GDPR and US privacy laws, have existing systems in place that may need only slight adjustments.

In contrast, micro, small, and medium enterprises (MSMEs) may need to invest more capital and resources to meet the legislation's requirements. Additionally, the lack of clarity in the rules creates uncertainty, making it challenging to budget for compliance costs. One stakeholder noted that certain legacy businesses, such as those in the banking or retail sectors, may not qualify as MSMEs but still face hurdles in implementing the DPDP Act due to resource constraints.

A staggered implementation of the DPDP Act, tailored to the size, scale, and nature of industries, could be a viable option to explore. However, such an approach must follow open consultations with stakeholders, including civil society, consumer groups, the private sector, and the government, to ensure inclusivity and effectiveness.

There is also near consensus on the heightened sensitivity of biometric data and an acknowledgement that the risks associated with it are higher. Biometric data is increasingly being used for routine activities such as employee attendance, airport security checks, and in classrooms. This widespread use raises the potential for identity theft, unauthorised monitoring, and discrimination, underscoring the need for stricter safeguards around its collection and use.[15]

Global Benchmarking

The EU's GDPR has long been regarded as the global standard for data protection and privacy regulations, specifically classifying biometric data as a subset of sensitive personal data. The GDPR defines biometric data "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data."[16] Article 9 of the GDPR affords additional protections to certain types of personal information, including biometric data, by recognising its sensitivity. Biometric data used to uniquely identify individuals is subject to strict regulations. According to guidance from the UK's Information Commissioner's Office (ICO), biometric data is considered personal information; if an organisation cannot justify its use with a valid reason, it must refrain from processing it. Even with a valid reason, the organisation must comply with all relevant data protection principles to ensure lawful processing.[17]

In contrast to the EU, the United States lacks a singular, federal privacy and data protection law. Instead, states such as California, Illinois, and Texas have implemented their own laws governing the collection and use of biometric data. These laws generally require companies operating in these states to obtain opt-in consent for collecting biometric information. Among these, Illinois's Biometric Information Privacy Act (BIPA) stands out due to its private right of action, which allows individuals to sue companies for violations even without having to prove direct harm. BIPA has gained attention with high-profile cases such as Facebook's US$650-million settlement in 2020, following accusations that the platform was using facial recognition technology to "tag" user photos without obtaining explicit consent, in violation of the BIPA. Similarly, lawsuits were filed against Microsoft, Google, and Amazon in 2019 for allegedly using Illinois residents' facial data to train facial recognition systems without consent.[18] However, recent amendments to BIPA

have slightly alleviated the pressure on companies. As of May 2023, businesses can now be held liable for only a single violation per person rather than for each instance of biometric data misuse. This amendment aims to limit excessive penalties while still holding companies accountable for privacy violations.[19]

Meanwhile, under China's Personal Information Protection Law (PIPL), biometric data is regarded as sensitive personal data.[20] Personal information processors can process sensitive personal information only when they have a specific purpose and sufficient necessity, and strict protective measures and consent of the individual has to be obtained prior to processing sensitive personal data.[21]

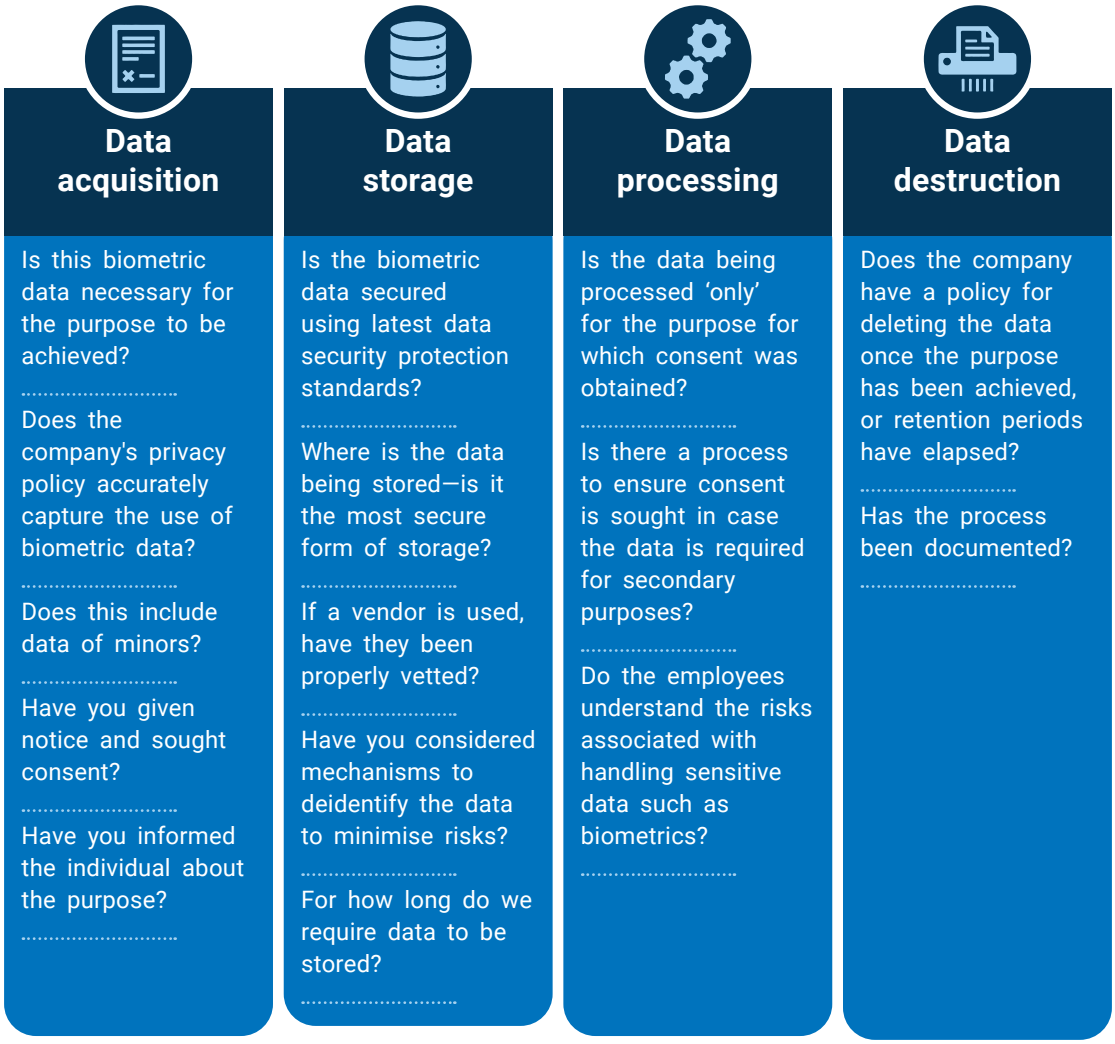
Best Practices for Secure and Transparent Biometric Data Processing

Best practices for collecting and processing biometric data are essential to ensure privacy and security. Entities handling such sensitive data must adhere to the following guiding principles:

- **Transparent Privacy Policies:** The company's public-facing privacy policy should clearly and honestly disclose its use of biometric data.
- **Detailed Biometric Data Policy:** The company's internal policy should provide comprehensive information on the types of biometric data collected, the purposes of collection, and potential uses.
- **Robust Data Security:** Biometric data should be secured using advanced data protection technologies. Independent third-party audits should be regularly conducted to verify the effectiveness of security measures.
- **Vendor Vetting:** If a third-party vendor is involved, the company should carefully vet them and document the security protocols implemented by the vendor for internal auditing purposes.
- **Risk Awareness Training:** Teams that handle biometric data should be fully aware of the risks associated with data breaches and understand the potential harms to individuals' privacy.

Following these practices can help build trust, mitigate risks, and maintain compliance with evolving data protection standards.

Figure 1: Factors to Consider when Collecting Biometric Data



Recommendations and Conclusion

Detailed Guidelines

Industry stakeholders emphasise that the lack of comprehensive guidelines from the government creates regulatory uncertainty, hindering small-scale industries in planning for the legislation's implementation. There is near consensus that the unique nature and immutability of biometric data increases the risks and harms associated with data breaches. Therefore, the government should adopt a harm-based approach for enforcement and impose stricter penalties for such breaches. MeitY must also release detailed guidelines on biometric data governance. Other jurisdictions, such as the ICO in the UK, have published extensive guidelines on biometric data governance and best practices that the Indian government should consider,[22] particularly with regard to the sensitivity of biometric data and mandating higher protection standards.

The Development of Reasonable Security Practices

The DPDP Act requires organisations collecting or processing personal data to implement reasonable security safeguards.[23] Business and industry organisations must establish robust security practices to protect biometric assets. Privacy by design should be the default, through integrating appropriate privacy-enhancing measures.[24] Additionally, the industry needs to develop technical standards that incorporate privacy and human rights. Standard-setting organisations, both domestically (e.g., Bureau of Indian Standards) and internationally (e.g., International Standards Organisation), should include representatives from the technology sector, ethics, civil society organisations, and academia.

Periodic Monitoring

Industry representatives indicate that they need more time to comply with the DPDP Act. The government should consider a staggered implementation of the law, allowing entities time to comply based on their size, nature, and capacity. Until compliance is achieved, these entities should report their progress to the Data Protection Board to demonstrate that they are taking adequate steps toward compliance.

Data Protection Impact Assessments (DPIAs)

Entities must conduct DPIAs to evaluate the risks associated with processing biometric data. In addition to periodic risk assessments, organisations should carry out DPIAs before ideating any new product.

Establishing Interdisciplinary Teams

Organisations should form interdisciplinary teams that include lawyers, technologists, ethicists, and security personnel to foster a culture that prioritises privacy within the organisation.

Isha Suri is Research Lead, CIS.

Pallavi Bedi is Senior Researcher, CIS.

Endnotes

1 UK Information Commissioner's Office, *Biometric Recognition Guidance: Impact Assessment*, 2024, biometric-recognition-guidance-impact-assessment-2024-02-22.pdf (ico.org.uk)

2 Frost & Sullivan, *India Biometric Market*, December 2010, https://store.frost.com/indian-biometric-market.html

3 Section 2(b), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, (2011).

4 Office of the Privacy Commissioner of Canada, *Data At Your Fingertips Biometrics and the Challenges To Privacy*, March 1, 2022, https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/.

5 Prasanth Aby Thomas, "Data Leak Exposes Personal Data of Indian Military and Police," CSO, May 2024, https://www.csoonline.com/article/2127645/data-leak-exposes-personal-data-of-indian-military-and-police.html

6 Matt Burgess, "A Leak Of Biometric Police Data Is a Sign Of Things To Come," *WIRED*, May 2024, https://www.wired.com/story/police-face-recognition-biometrics-leak-india/.

7 "MHA Warns Against Cybercriminals Posing As Police Officials," *ET Prime*, May 2024, https://economictimes.indiatimes.com/news/defence/mha-warns-against-cybercriminals-posing-as-police-officials/articleshow/110126470.cms?from=mdr.

8 Kuber Singh, "70:30 Partnership Offered By Gujarat To Societies For CCTV Camera Installation," *Security Today*, November 2014, https://www.securitytoday.in/7030-partnership-offered-by-gujarat-to-societies-for-cctv-camera-installation/.

9 "Delhi Government To Subsidise Power For CCTVs Outside Homes," *Times of India*, June 2019, https://timesofindia.indiatimes.com/city/delhi/delhi-government-to-subsidise-power-for-cctvs-outside-homes/articleshow/69718926.cms.

10 Office of the Privacy Commissioner of Canada, *Data At Your Fingertips Biometrics and the Challenges To Privacy*.

11 Section 43, Information Technology Act, 2000.

12 Amber Sinha, "The Landscape Of Facial Recognition Technologies In India," *TechPolicy Press,* March 2024, https://www.techpolicy.press/the-landscape-of-facial-recognition-technologies-in-india/.

13 PRS Legislative Research, *The Digital Personal Data Protection Bill,* 2023, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023.

14 The Digital Personal Data Protection Bill, 2023

15 Shlok Sharma, "The Irreversible Footprint: Biometric Data and the Urgent Need For Right To Be Forgotten," *Bar and Bench*, August 2024, https://www.barandbench.com/columns/the-irreversible-footprint-biometric-data-and-the-urgent-need-for-right-to-be-forgotten.

16 Article 4(14), General Data Protection Regulation, EU 2016/679.

17 Information Commissioner's Office, Government of United Kingdom, *How Do We Process Biometric Data Lawfully?*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/.

18 JB Schiller, "Biometrics Regulations: Navigating US Biometric Laws," *Goodwin*, Nov 8, 2021, https://www.goodwinlaw.com/en/insights/blogs/2021/11/biometrics-regulations-navigating-us-biometric-law

19 BIPA-Procedure-Damages, Bill Status of SB2979, https://www.ilga.gov/legislation/BillStatus.asp?DocNum=2979&GAID=17&DocTypeID=SB&LegId=152094&SessionID=112&GA=103.

20 Article 28, The China Personal Information Protection Law.

21 Article 29, The China Personal Information Protection Law.

22 Information Commissioner's Office, Government of United Kingdom, *How Do We Process Biometric Data Lawfully?*

23 Section 8(5), The Digital Personal Data Protection Act.

24 Centre for Information Policy Leadership, *Privacy-Enhancing and Privacy Preserving Technologies: Understanding the Role Of PETs and PPTs In the Digital Age*, December 2023, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf.

Key Takeaways

Basu Chandola

The application of biometric solutions is increasing in different parts of the world, with fingerprint mapping, facial recognition, and retina scans becoming common in smartphones, airport security, financial services, workplace security, and shopping. Such widespread use of biometric solutions raises serious privacy and data protection concerns, as biometrics rely on human body characteristics and biological traits that cannot be changed or separated from the data principals.[1] Consequently, the risks associated with biometric data are significantly higher than those of other data categories, warranting stricter regulations.

Jurisdictions worldwide place stricter scrutiny on the processing of biometric data. The European Union's (EU) General Data Protection Regulation (GDPR) requires explicit consent[2]—which has a higher threshold than general consent—for

processing biometric data and grants individuals rights against automated decision-making.[3] Similarly, countries like Canada,[4] South Africa,[5] Australia,[6] and China[7] classify biometric data as sensitive personal information and enforce stricter regulations.

Challenges, Implementation, and Impact

Under the prevailing Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (IT Rules), biometric data is classified as "sensitive personal information".[8] It is defined as "technologies that measure and analyse human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements, and DNA for authentication purposes."[9] Organisations processing, handling, or dealing with such data must follow reasonable security practices and procedures. However, the Digital Personal Data Protection Act, 2023 does not define sensitive personal data and treats all types of personal data similarly. At first glance, this approach contrasts with regulatory frameworks in other jurisdictions.

Under the DPDP Act, biometric data, like other types of personal data, can only be processed for a lawful purpose for which the data principal has provided consent or for certain legitimate uses. The consent provided by the data principal must be "free, specific, informed, unconditional, and unambiguous, with a clear affirmative action,"[10] demonstrating that the data principal agrees to the processing of their personal data for the specified purpose. The request for such consent must inform the data principal about the data being collected, the purpose of the collection, the process for withdrawing consent, the grievance redressal process, and how to file a complaint with the Data Protection Board of India.

While the DPDP Act does not further categorise personal data, Section 10 of the Act encapsulates the concept of varying sensitivity levels. This section empowers the Central Government to designate any data fiduciary or class of data fiduciaries as a Significant Data Fiduciary (SDF) based on several factors, including the "volume and sensitivity of personal data processed."[11]

SDFs must comply with additional obligations, including appointing a Data Protection Officer, engaging an independent data auditor to conduct data audits, performing periodic Data Protection Impact Assessments, and undergoing regular audits, along with any other measures that may be prescribed.[12]

Thus, the DPDP Act allows data fiduciaries processing certain types of sensitive data to be granted special status and to be subject to additional obligations.[13] Given the sensitive nature of biometric data and the high risks associated with its breach, it can easily qualify for the SDF category.[14] Consequently, separate rules governing biometric data can be

established to enforce higher standards for its storage, deletion, and protection.[15]

The IT Act has defined sensitive personal data as "personal information as may be prescribed by the Central Government"; further classifications of different types of personal data, including biometric data, were established by the IT Rules. A similar approach is being adopted under the DPDP Act, where the Act outlines broader principles, while specific details will be defined later through secondary legislation.

If data fiduciaries processing biometric data do not qualify as SDF, strict interpretations must apply. A high consent threshold must be maintained to ensure that data principals can make informed decisions and avoid potential harms. Consent, rather than legitimate use, should serve as the basis for processing biometric data, and data principals must have the option to refuse non-essential processing.

Implementation Recommendations

Although the DPDP Act was enacted in August 2023, the provisions of the Act are yet to be notified.[a,16] As of writing, the Ministry of Electronics and Information Technology (MeitY) is developing the Digital Personal Data Protection Rules, soon to be released for public consultation.[17] However, delays have created regulatory uncertainty for businesses and citizens.[18] To ensure clarity and successful implementation of the DPDP Act regarding biometric data, the following points must be considered:

- The DPDP Rules should clarify the regulation of biometric data and establish stricter obligations for its processing. Efforts must focus on harmonising these obligations with those in other leading jurisdictions.
- MeitY should conduct extensive public consultations with various stakeholders to finalise the DPDP Rules. Specific consultations with data fiduciaries handling biometric data are essential for understanding the industry's perspective.
- The provisions of the DPDP Act must be notified in a phased manner, allowing data fiduciaries sufficient time to implement the obligations in their businesses.
- The government must take steps to clarify the application of the DPDP Act to biometric data. The lack of clarity complicates budgeting for compliance and developing expertise within businesses.

---

[a] As of 10 September 2024.

- A harms-based approach to regulating biometric data must be adopted by the government.
- The industry should strive to develop and incorporate technical standards that prioritise privacy in their practices by deploying privacy-enhancing measures.
- Strict interpretation and implementation of the DPDP Act concerning biometric data must be observed.

Conclusion

The use of biometric data holds immense potential, even as it carried significant risks. While the existing IT Act provides guidance on regulating biometric data, the newly enacted DPDP Act leaves plenty of issues open to interpretation and relies on secondary legislation for finalisation. In the absence of DPDP Rules, the industry experiences regulatory uncertainty. It is crucial to develop specific rules for biometric data to ensure the protection of citizens' rights and to minimise associated risks and harms.

Basu Chandola is Associate Fellow, ORF.

Endnotes

1 C. Wendehorst and Y Duller, *Biometric Recognition and Behavioural Detection,* Brussels, European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf .

2 General Data Protection Regulation, Article 9-Processing of Special Categories of Personal Data, https://gdpr-info.eu/art-9-gdpr/

3 General Data Protection Regulation, Article 22-Automated Individual Decision-making, Including Profiling, https://gdpr-info.eu/art-22-gdpr/.

4 Sasha Coutu, "Privacy Commissioner of Canada Updates Guidance Regarding Sensitive Personal Information," *Dentons Data,* August 19, 2021, https://www.dentonsdata.com/privacy-commissioner-of-canada-updates-guidance-regarding-sensitive-personal-information/.

5 South Africa's Protection of Personal Information Act, 2023, Section 26, https://popia.co.za/section-26-prohibition-on-processing-of-special-personal-information/

6 Australia's The Privacy Act 1988, Section 6, https://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/pa1988108/s6.html

7 China's Personal Information Protection Law 2021, Article 28, https://personalinformationprotectionlaw.com/PIPL/article-28/

8 The Information Technology Act, 2000, Section 43A, Explanation iii.

9 The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Rule 2A.

10 Digital Personal Data Protection Act, Section 6, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

11 Digital Personal Data Protection Act, Section 10, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

12 Digital Personal Data Protection Act, Section 10, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

13 Ramya Khanna, "Personal Health Data Under the Digital Personal Data Protection Act, 2023: Private and Esoteric?," *The CCG Blog,* February 13, 2024, https://ccgnludelhi.wordpress.com/2024/02/13/personal-health-data-under-the-digital-personal-data-protection-act-2023-private-and-esoteric/ .

14 Vijayashankar Na, "Who is or Who Should be a Significant Data Fiduciary?," *Naavi*, June 17, 2024, https://www.naavi.org/wp/who-is-or-who-should-be-a-significant-data-fiduciary/; King Stubb & Kasiva, "Regulation of Biometric Data Under the Digital Personal Data Protection Act, 2023," November 2, 2023, https://ksandk.com/data-protection-and-data-privacy/regulation-of-biometric-data-under-the-dpdp-act/# .

15 Shlok Sharma, "The Irreversible Footprint: Biometric Data and the Urgent Need for Right to Be Forgotten," *Bar and Bench,* August 9, 2024, https://www.barandbench.com/columns/the-irreversible-footprint-biometric-data-and-the-urgent-need-for-right-to-be-forgotten# .

16 India Briefing, April 30, 2024, https://www.india-briefing.com/news/india-dpdp-act-to-be-enacted-after-2024-general-elections-32269.html/; Pranay Manek, "India's New Data Protection Act, DPDPA, Is Coming — Is Your Business Ready?," *Barracuda*, June 13, 2024, https://blog.barracuda.com/2024/06/13/india-data-protection-act-dpdpa# .

17 Aroon Deep, "Rules for Data Protection Act Within One Month: Vaishnaw," *The Hindu,* August 19, 2024, https://www.thehindu.com/news/national/rules-for-data-protection-act-within-one-month-vaishnaw/article68543611.ece .

18 Ashutosh Mishra, "One Year of DPDP Act: Firms in a Fix Over Delayed Implementation of Rules," *Business Standard,* August 11, 2024, https://www.business-standard.com/economy/news/one-year-of-dpdp-act-delayed-rules-hamper-india-s-data-protection-law-124081100299_1.html .

02

FINANCIAL DATA

Academic Perspective

Gowree Gokhale and Ayush Tripathi

The fintech industry in India has grown in the last decade, and especially during the previous five years; today the country has the highest fintech adoption rate in the world at 87 percent.[1] The use of technology in finance and payments has revolutionised the banking and financial services industry, changing the way in which consumers access finance while also compelling the traditional banking industry to adopt digital mediums and innovate to remain competitive. In terms of market size, India is the fastest growing fintech market in the world, with current market size estimated to be around US$110 billion and projected to reach US$420 billion at a CAGR of 31 percent by 2029.[2] In the year 2023-24, the number of digital transactions in the country was estimated at around 185 billion,[3] with the volume of transactions crossing INR 20 trillion every month between May to November 2024.[4] The overall

health of the fintech sector can also be seen in the growth of fintech startups in the country—from 2,100 in 2021 to 10,200 in 2024.[5] A critical driver of this growth is the ability of fintech startups to harness and process large datasets, be it for innovation, targeted products and solutions, and fraud detection.

Data protection activities in the Banking Financial Services and Insurance (BFSI) sector are regulated by the Information Technology Act, 2000 and allied rules as well as sectoral regulations by the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India (IRDAI), and the Security Exchange Board of India (SEBI). With the enactment of the Digital Personal Data Protection Act, 2023, the finance industry finds itself at a point where they have to rework their business model to ensure compliance with the new legislation. It is also important to note that financial data is classified as 'sensitive personal data' under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.[6] Therefore, it is important to assess the potential conflicts and overlaps that have to be streamlined between horizontal and sectoral laws to ensure the sustained growth of the industry.

Challenges, Implementation, and Impact

There are certain areas of fintech that sectoral regulators do not regulate directly, as they have the mandate to regulate only Regulated Entities (REs). These include outsourcing entities and digital lending apps, which are indirectly regulated by RBI through REs. Therefore, although the DPDP Act will directly apply to them, they will have to continue adhering to sectoral laws.

Determining Data Fiduciaries and Data Processors

Under the DPDP Act, the obligation of compliance of the provisions is on data fiduciaries. In the banking and finance ecosystem, given that there are multiple stakeholders involved in facilitating the transactions, distinguishing data fiduciaries and data processors will be challenging. As per Section 2(i) of the DPDP Act, a data fiduciary is the person which determines the purpose and means of processing the data. However, in a transaction that goes through multiple stakeholders, with each stakeholder determining their own purpose and means, there are joint data fiduciaries who determine the purpose and means of processing. Therefore, imposing an obligation on each data fiduciary in a transaction to obtain consent will add to the burden of the entities.

For example, in case of digital lending, the borrower logs in to a digital lending application, which communicates the loan amount to authorised lenders, i.e., either the bank or Non-Banking Financial Companies (NBFCs). The authorised lenders then turn to lending service providers who then process the loans and send them through digital lending apps

and the borrower's bank to complete the process. In this situation, while the data is being collected by a digital lending app, only the loan service providers will be the data processors; the others will be categorised as data fiduciaries as their purpose and means of processing data may differ. Therefore, identification and compliances will differ based on the identification and role of the stakeholder involved, and each data fiduciary will have to obtain consent even if their operations are not consumer facing.

Consent, Collection, Handling, and Purpose Limitation

Besides the Master Directions on KYC and explicit consent under Digital Lending Guidelines, 2022 (DLG),[7] the industry has been operating on general broad-based consent mechanisms. As per Section 4 of DPDP Act, data fiduciaries can only process data either after obtaining consent or in some other legitimate cases mentioned in Section 7 of the Act.[8] Under the DPDP Act, a notice with purpose limitation and explicit action would be required to obtain consent.

In cases of financial transactions that are processed through multiple channels, it will need to be clear as to which entities are data fiduciaries and which are processors. In some cases, there may be joint data fiduciaries. Practically, entities that manage consumer-facing apps can provide and obtain consent. In card payments, for example, stakeholders include merchants, Payment Aggregators and Payment Gateways (PA/PGs), merchant banks, card networks, and payer's banks. These entities need to work together to ascertain who are the fiduciaries (or joint fiduciaries) and who are the processors, then ensure the implementation of appropriate notice and consent mechanisms that communicate the purpose of processing by each entity. There may be multiple levels of notice and consent.

In the Digital Lending Guidelines, Lending Service Providers (LSPs) are required to obtain explicit consent of the borrowers, and they are explicitly prohibited from accessing mobile phone resources like files and media, contact list, call logs, and telephony functions, regardless of consent.[9] The DPDP Act does not place any such restrictions as long as the notice and consent mechanism is followed. However, in view of Section 38 of the DPDP Act,[10] the obligations under the Act are in addition to the sectoral laws and not in derogation of them; therefore, a case can be made for aligning the sectoral regulations with horizontal law to provide leniency to digital lending companies.

Data Sharing

Financial services is a data-intensive industry that requires continuous data sharing with third parties for engagements. The DPDP Act confers strict obligations in terms of data sharing, where obtaining explicit consent from the data principal is mandatory. This obligation becomes more problematic in cases where data sharing

is mandated by law. While there is a legitimate exception for use in sections 5 and 7 of the Act, these exceptions only aid processing for purposes such as the sharing of KYC records under Prevention of Money Laundering Act (PMLA) or Insolvency and Bankruptcy Code (IBC) to help authorities check for money laundering and insolvency proceedings, respectively.

The same exceptions are not applicable on credit information companies and obligations under the Credit Information Companies (Regulation) Act, 2005.[11] Fintech regularly have to share borrowers' data with credit-scoping companies to determine and assess creditworthiness. This data sharing is governed by the Credit Information Companies (Regulation) Act, 2005 and overseen by the RBI. In case of a data principal evoking their right to refusal, the institutions will be stuck between the rights of the data principal and mandated data sharing by law.

Further, the banking and financial services industry, including banks and fintech companies, outsource most of their functions to third parties such as cloud service providers. In such cases, entities will have to ensure that the third parties comply with both the DPDP Act and the RBI's guidelines on the outsourcing of IT services. Further, under Clause 3.6 of the Information and Cyber Security Guidelines, 2023 of IRDAI,[12] InsurTech companies are required to ensure that any data shared with a third-party service provider must have a valid business purpose. Data generated by the third party during operations for the organisation will belong to the organisation and must adhere to its policies. When in the control of a third party, organisational data must be subject to the same or stricter controls based on its classification according to the Information Security (IS) policy. The organisation has the right to delete its information from vendor assets as per the data-retention policy and must receive all data back upon contract termination.

This will put an immense burden on regulated entities to comply with requirements under both the regulations and rules thereof.

Data Security and Breach

Data security is critical aspect to the banking and financial services industry, given the nature of data handled by them. The applicable security and data breach related provisions at present are the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules),[13] cyber security breach reporting to CERT-In[14] under the IT Act, and RBI's sectoral guidelines.[15]

Section 8(5) of the DPDP Act mandates that data fiduciaries have to protect the data of consumers and are also responsible for the data processors. This necessitates the pre-emptive classification of data fiduciaries and data processors in the financial sector to correctly attribute liabilities. Further, as the financial sector outsources most activities to third parties, i.e., data processors, there needs to be

clarity regarding the attribution of liability in cases where a data breach takes place at the processor's end.

Further, in cases of security breaches, there are overlapping strict reporting requirements from the RBI, CERT-In,[16] and now under Section 8(6) of the DPDP Act. The DPDP Act also provides for inquiry and imposition of penalty in such cases of data breach under Section 27(1) of the Act. For the entity that has suffered the cybersecurity attack, it could be burdensome to report to three different authorities within a limited amount of time. RBI and CERT-In require reporting within two to six hours and six hours, respectively. Adding another reporting requirement will add to the compliance burden. Therefore, the reporting requirements should be applicable to only those entities that are not covered through RBI's sectoral guidelines. Further, the concept of voluntary undertaking is not present in RBI's cybersecurity framework. Therefore, even if an entity services a voluntary undertaking to a data protection authority, it is not absolved under RBI's jurisdiction. There has to be a harmonisation of these laws to protect the interest of this industry from heavy compliance obligations.

Data Localisation

Data localisation is an area in which regulations get complicated. Under Directive RBI/2017-18/153, 2018,[17] Section 10(2) read with Section 18 of the Payment and Settlement Systems Act 2007, system providers have to ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data includes the full end-to-end transaction details and information collected, carried, or processed as part of the payment instructions.

Notably, Section 16 of the DPDP Act allows data transfers to the notified country. While Section 16 allows for sectoral laws to prevail over the DPDP Act, a case can be made for RBI to allow data transfers to notified countries under DPDP Act. While there can be various considerations behind data localisation by regulators and legislators, one of the key rationales behind data localisation is to secure the data of individuals, i.e., considering data is more private and secure if stored within the country. However, some research has shown that data localisation does not translate to high commercial privacy and data security standards.[18] Additionally, it needs to be understood that the security of data is not a function of where it is stored. Besides, as many business entities have a "legal nexus", they cannot escape a nation's regulatory mandate despite storing data overseas.

Thus, data security and privacy are agnostic to the location of the data server and more dependent on principles and standards. Further, in the absence of a definition of financial and non-financial data, the entities have to keep all the data in India to ensure compliance, which could be burdensome. Another rationale given in favour of data localisation is the ease of access to data for law enforcement purposes. There is a growing belief that

if the data is stored outside the country, regulators will face difficulty in accessing that data. However, through bilateral and multilateral frameworks, including the Mutual Legal Assistance Treaty and other regional agreements, the law enforcement agencies can gain access to data stored abroad. Towards this, RBI should consider relaxing the data localisation norms to harmonise them with the DPDP Act and ensure coherence in data-storage norms.

Implementation Recommendations

The financial sector is one of the most heavily regulated sectors in India. RBI, SEBI, IRDAI have been proactive in terms of regulation and protection of data. This is evident in RBI's recent actions against prominent banks and fintech for their lack of compliance in terms of cybersecurity. If another legislation has to be implemented, it must be harmonised with the existing regulations and tailored to the needs of the sector.

There is a need for in-depth deliberations before the rule-making process to harmonise the horizontal law and sectoral law to streamline compliance. The overlaps and inconsistencies between the two may create additional compliance burdens for financial entities, which could prove detrimental, especially for startups. Even though this sector handles sensitive data, a case could be to harmonise sectoral norms with horizontal law and provide leniency at places where there are overlaps and inconsistencies in favour of ease of compliance burden. In consent, there is a need to avoid duplicity of procedural laws. For instance, the mandatory obligation of obtaining consent should be implemented at the first instance when the consumer interacts with the application and therefore the obligation should be on the data fiduciary running the application. This is as long as the said fiduciary is making full disclosures with regard to the means and purposes defined by other fiduciaries involved in the transactions.

In light of the above challenges, it is recommended that policymakers review both sectoral laws and the DPDP Act to build a single framework for compliance for financial entities and revisit some of the stringent norms that currently exist to ease the burden of entities.

Gowree Gokhale is an independent legal counsel and advisor.

Ayush Tripathi is Senior Programme Manager, Digital Economy Vertical, The Dialogue.

Endnotes

1 Ministry of Commerce and Industry, Government of India, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1759602.

2 Ajay Kumar Chaudhary, "Fintech Sector – Catalyst to Growth" (Keynote Address, New Delhi, July 18, 2024), https://www.npci.org.in/PDF/npci/chairman-speeches/2024/Special-Keynote-Address-delivered-by-Shri-Ajay-Kumar-Choudhary-Non-Executive-Chairman-and-Independent-Director.pdf?TSPD_101_R0=08f002952bab2000553b7d0641a59e1bdf7198659b28be043d478527eb8185ca4563618a353659ad08e812aa93143000a96ae394208e790c4169b07f1ba3f48a7835b64f00185edc734c64a46fa90178ec6aceab8938e9e9e7be0679d0258411.

3 Kanishk Sarkar et.al., *The Indian Payments Handbook 2024-2029,* PwC, 2024 https://www.pwc.in/assets/pdfs/indian-payment_handbook-2024.pdf.

4 Product Statistics, "National Payment Corporation of India," https://www.npci.org.in/what-we-do/upi/product-statistics.

5 Indian Brand Equity Foundation, "India home to 26 fintech unicorns with a combined market value of US$ 90 billion," 2024, https://www.ibef.org/news/india-home-to-26-fintech-unicorns-with-a-combined-market-value-of-us-90-billion.

6 Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 s 3.

7 Reserve Bank of India, "Guidelines on Digital Lending," 2022, https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12382&Mode=0.

8 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 7," 2023.

9 Reserve Bank of India, "Guidelines on Digital Lending- section 10.1," 2022.

10 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 38," 2023.

11 Indian Code, "Credit Information Companies (Regulation) Act, 2005," https://www.indiacode.nic.in/bitstream/123456789/2057/2/A200530.pdf

12 IRDAI, "Information and Cyber Security Guidelines, 2023," https://irdai.gov.in/document-detail?documentId=3314780

13 The Information Technology (reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

14 Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet, No. 20(3)/2022-CERT-In, https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf.

15 Reserve Bank of India, "Cyber Security Framework in Banks," https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0.

16 Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet, No. 20(3)/2022-CERT-In, https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf.

17 Reserve Bank of India, "Storage of Payment System Data," https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0.

18 Daniel Castro, "The False Promise of Data Nationalism," The Information Technology & Innovation Foundation, December 2013, https://www2.itif.org/2013-false-promise-data-nationalism.pdf.

An Application Perspective

Hardeep Singh

Over the past decade, the financial services industry has emerged as a cornerstone of India's economic growth. India is a success story, from record profits in the banking sector[1] to the expansion of credit disbursement[2] and the remarkable success of the payments ecosystem.[3]

Much of this achievement has been driven by a collaborative push from financial regulators and the Indian government, supported by affordable mobile phones and low-cost data. The launch of the Unified Payments Interface (UPI) instant payment system sparked a digital revolution in the financial services sector, bringing around three billion UPI users into the financial ecosystem in the recent years.[4] A crucial component of this transformation is identity verification, an area in which India is a global leader. Video-enabled 'know your customer' (KYC)

processes, supported by a centralised digital stack (Digital KYC), are the first step in accessing financial services and promoting financial inclusion.

The financial technology (fintech) boom, which builds on this foundation, has empowered startups to offer personalised financial products across all sectors. For instance, with digital public infrastructure (DPI), personal loans can be disbursed into users' bank accounts within minutes, and bills (such as electricity, utilities, or credit cards) can be settled in real-time. On the investment front, DPI enables daily settlements in equity cycles, marking a world's-first for such a system.

Today, users are expanding their digital presence by accessing various financial services online. These include lending and payment services regulated by the Reserve Bank of India (RBI), investments in equities and mutual funds through brokers and investment advisors registered with the Securities & Exchange Board of India (SEBI), and insurance policies regulated by the Insurance Regulatory & Development Authority of India (IRDAI).

Industry Standards and Expectations

Fintech apps are pivotal in shaping today's digital ecosystem, acting as the distribution layer for regulated entities (REs) across all financial regulators like SEBI, RBI, and IRDAI. Until recently, each regulator drafted data protection rules within their specific context—RBI embedded them in broader lending and payment guidelines, SEBI included them in directives for brokers and advisors, and IRDAI did the same for insurers. However, fintech firms operating across the entire financial spectrum had to navigate varied regulations based on the entities they partnered with, leading to inconsistency and complexity.

A related challenge is that despite the scale of fintech firms, they were only indirectly regulated by financial authorities, as parliamentary statutes limited direct oversight to REs. This regulatory structure imposed specific compliance obligations on REs, who were responsible for auditing and ensuring that their fintech partners adhered to data protection guidelines, such as the RBI's Digital Lending Guidelines (DLG)[5] or PA Guidelines.[6] As a result, each RE had to enforce compliance individually, creating operational burdens for the REs and their fintech partners.

This approach may have had the right intention, but was not suited to the scale at which fintechs were operating. Since most such firms partnered with multiple REs, each RE conducted annual audits on the fintech partners. The sectoral regulators' broadly worded rules often led each RE to interpret data protection requirements differently. As a result, fintech firms faced duplicated efforts and costs, as each RE audited them based on its understanding, despite checking for similar compliance aspects.

India's digital boom highlighted the need for a more refined approach to data protection. Although sectoral regulators remained vigilant, the scale of fintech growth called for a comprehensive review. This prompted the government to introduce the first draft of the Personal Data Protection Bill in 2018. After several consultations, joint parliamentary committee reviews, and a revised Bill in 2022, the new Digital Personal Data Protection (DPDP) Act was passed on 11 August 2023.

The DPDPA's most significant contribution to the financial services industry is creating an enabling environment, a standardised taxonomy, and a clear framework of rights and responsibilities for intermediaries. With this Act, the financial services sector now benefits from a unified approach to compliance; fintech firms can adhere to a universal standard for data protection rather than catering to the varying demands of individual REs.

Data Protection: Challenges, Implementation, and Impact

The data lifecycle is typically divided into six parts[7]—planning, capture, management, analysis, archiving, and destruction. The DPDPA addresses all stages comprehensively.

- Planning and Capture: At this stage, the data fiduciary determines the grounds for processing data, notifies the data principal, and obtains consent for a specific, limited purpose. Here, the principles of data governance are also established to decide data storage based on the criticality and sensitivity of the data. The DPDPA covers these aspects under Section 4 (Grounds for processing personal data), Section 5 (Notice), and Section 6 (Consent), ensuring that data is collected responsibly and with transparency.
- Manage and Analyse: Once the data is captured, the data fiduciary must implement technical safeguards to manage the data, ensuring its protection against breaches. This stage also involves analysing data to identify trends and insights that drive business decisions. Moreover, onward data sharing is governed by classifications established during the planning phase. The DPDPA addresses these responsibilities under Section 8 (General obligations of Data Fiduciary), Section 9 (Processing of personal data of children), Section 10 (Additional obligations for significant data fiduciaries), and Chapter III, which outlines the broader obligations for handling and analysing personal data responsibly.
- Archive and Destroy: At this stage, the data is no longer needed for daily operations but may still hold importance for legal, compliance, or future reference purposes. The focus is on securely archiving the data to prevent unauthorised access to sensitive information. Once the data fiduciary determines that the data is no longer useful and is not required for legal or compliance reasons,

it must be securely deleted. This step ensures that data is not stored indefinitely, mitigating the risk of unauthorised access or breaches. The DPDPA reinforces these principles by laying out data retention and deletion guidelines, ensuring that data is managed responsibly even at the end of its lifecycle.

Additionally, the DPDPA establishes a direct relationship between the consumer and fintechs/REs concerning the processing of personal data. This increases the accountability of fintechs and REs in handling consumer data, creating a clear pathway for consumers to understand how their data is used and processed. The Act also provides a remedial framework, enabling consumers to assert their rights and seek redress if fintechs or REs violate their data privacy. This fills a critical gap in the regulatory landscape, complementing the frameworks set by sectoral regulators by ensuring uniform data protection standards and reinforcing consumer rights across the financial ecosystem.

Prior to the DPDPA, India's data protection framework lacked the nuanced approach required for uniform implementation. The multiplicity of guidelines across different financial regulators created challenges for the sector, resulting in overlapping and sometimes conflicting compliance requirements. The DPDPA expands and reinforces many obligations already imposed on REs and their fintech partners. However, its key contribution is the clarity it provides through detailed illustrations and explanations within the Act. This helps streamline compliance efforts and complements the existing regulatory ecosystem, ultimately reducing the compliance burden to some extent.

For instance, consider the data deletion requirement, which is a part of the DLG Guidelines[8] and the DPDPA. The DPDPA, following multiple rounds of consultations, introduced much-needed nuance to this requirement. Section 12(3), read along with Section 38(2),[9] allows a data fiduciary to retain personal data even if a deletion request is made, provided it is necessary for a specified purpose or to comply with other laws. This clarification was crucial for fintech players and REs, as the DLG Guidelines did not offer such an exception.[10] Section 6(6) also empowers data fiduciaries to continue processing personal data if required by law, even if the data principal withdraws consent.

In the financial services context, broader laws such as the Prevention of Money Laundering Act or Information Technology (IT) Rules mandate that data be stored and processed for up to 10 years. Before the DPDPA, sectoral guidelines did not explicitly allow for this exception, leading to confusion among REs and fintech players about whether to prioritise the deletion of data or compliance with other Acts and rules. The DPDPA resolves this ambiguity by providing clear exclusions and harmonising data retention practices with broader legal requirements.

Another positive impact of the DPDPA is the establishment of a standard taxonomy and framework. This framework delineates the roles and responsibilities of all parties involved in a financial transaction.

For instance, when fintechs partner with REs to offer loans, fintechs operate as loan service providers (LSPs) under the DLG Guidelines. In this arrangement, the RE provides the loan and maintains the primary relationship with the end user, designating the RE as the "data fiduciary."[11]

Before the enactment of the DPDPA, the nature of the relationship between the LSP and the user was often ambiguous and open to interpretation. These relationships were frequently negotiated within contracts between the LSP and the RE, leading to variability across different partnerships. This inconsistency directly affected how LSPs processed user data, particularly concerning clauses related to data deletion, retention, and cross-selling practices. The DPDPA's clear framework mitigates this ambiguity, ensuring more uniformity and compliance across the sector.

The DPDPA acknowledges and clarifies the relationship between the LSP and the user. In this framework, any data that the LSP consensually collects as part of its principal relationship with the user—where the user engages with various tech services offered by the LSP—belongs to the LSP itself. Thus, in this context, the LSP is designated as the 'data fiduciary'.

As the data fiduciary, the LSP has the authority to process and utilise the data for the purposes for which consent was obtained. Conversely, the data that is collected, processed, and stored in connection with the specific financial services offered by the RE (through the fintech firm) is considered the property of the RE. In this case, the RE is classified as the data fiduciary for that data. This clear delineation of responsibilities enhances accountability and ensures that both LSPs and REs can operate within a defined legal framework regarding data handling and user consent.

Notably, the LSP and the RE relationships will emerge and coexist simultaneously within the same transaction, albeit in the context of different data sets. In this scenario, both data fiduciaries will bear parallel obligations under the DPDPA corresponding to the different data sets they manage.

Establishing a dedicated data privacy regulator as per the Act[12] aims to enable investigating breaches, addressing grievances, initiating inquiries, and imposing fines, mirroring the regulatory structure of the European Union's General Data Protection Regulation. The Act aligns with global norms in terms of the coverage and grounds for processing personal data. For instance, it permits private data fiduciaries to process personal data solely through two means: (i) consent or (ii) specifically defined 'legitimate uses'. Individual rights granted to data fiduciaries, such as the right to be

forgotten and the right to correction, are also inspired by global data protection regulations.

However, there are areas where a different approach would have been preferable. In some instances, the framework is overly prescriptive compared to the collective global experience. A notable example is the consent framework, where the Act includes an illustration recommending the automatic expunging of consent.[13] The idea of a data principal's ownership and consent over their data is central to the Act. Once the user provides consent—after thoroughly reviewing and understanding the consent screen, which outlines the purpose and relevant details—this should be deemed final. The illustration suggesting the automatic rejection of consent or portions of consent, along with the mandated auto-deletion of data, undermines the foundational concept of informed consent.

Determining what constitutes a key service provided by an app is a nuanced challenge. For instance, the financial services sector currently grapples with significant issues surrounding increasing fraud. Many key fintech players are integrating fraud prevention services into their core offerings. These services, akin to value-added services, often necessitate access to additional data, such as SMS or contact lists. While this SMS/contact list data might not be directly essential for the primary service, it plays a critical role in fraud prevention, safeguarding both users and systems. Given that consent is the central theme of the DPDPA, once a data principal provides informed consent, it seems unjust to revoke that consent automatically on the grounds that SMS/contact lists are unnecessary, primarily when assessed by a third party that may lack a comprehensive understanding of the sector and the importance of fraud prevention.

Another pertinent issue within the lending ecosystem is the omission of 'enforcement and collection of debt' from the current framing of Section 7. Without the specific inclusion of this 'end-use', REs and LSPs face the risk that while data principals may consent to data processing for underwriting and loan disbursal, they might explicitly deny consent for sharing their data with third-party collection agents for collections and follow-ups.[14] For instance, the collection of debt—particularly distressed debt—is often outsourced to third-party collection agents.

This arrangement represents an efficient division of labour, as REs and LSPs possess different skill sets than those required for debt recovery. If these entities cannot outsource this function, they may adopt a more conservative approach to credit assessments, potentially excluding the 'thin-file' borrower cohort altogether. Such a shift could lead to welfare losses for these borrowers.

Despite these concerns, the DPDPA is among the most promising legislation introduced in India in recent years. Notably, the legislative process—though lengthy—was commendable for incorporating

feedback from numerous consultations and parliamentary debates. The industry has high hopes for the DPDPA, especially alongside the forthcoming Digital India Act.

Conclusion

An expectation from the forthcoming Digital India Act is respecting the due process rights of recognised fintechs and REs before enforcing measures such as removing access to websites or applications from app stores. This expectation arose from experiences in 2023 when certain enforcement actions were executed without adequately distinguishing between good and bad actors, resulting in collateral damage to legitimate fintech companies and regulated entities.

The Digital India Act is an upgrade of the outdated IT Act, making it a welcome development. India's digital ecosystem has evolved considerably since the IT Act was enacted in the 1990s. Therefore, enforcement measures must be carefully calibrated. Without the growth and innovation fostered by the trust established through the DPDPA, these advantages could be jeopardised by an overly strict and punitive enforcement approach under the Digital India Act.

In conclusion, the DPDPA enhances the protections available to its subjects across several key stages of the data cycle. It reinforces a rights-based framework, offering a remedial forum stronger than existing sectoral options, such as an ombudsman. Moreover, by establishing a clear taxonomy of intermediaries processing data and articulating their rights and obligations, it indirectly fosters innovation by allowing certain intermediaries to access sector-specific datasets that were previously unavailable to them.

Hardeep Singh is Head of Legal and Government & Regulatory Engagement Function, CRED.

Endnotes

1 Press Trust of India and Business Standard. "Public Sector Banks' Total Profit Jumps 35%, Crosses Rs 1.4 Trn in FY24." *Business Standard,* May 14, 2024. https://www.business-standard.com/finance/news/public-sector-banks-total-profit-jumps-35-crosses-rs-1-4-trn-in-fy24-124051400505_1.html

2 Deepak Bagla et al., "A Review of India's Credit Ecosystem," *Invest India (2021),* https://experian.in/wp-content/uploads/sites/27/2023/05/Experian-Invest-India-Report-A-Review-of-Indias-Credit-Ecosystem.pdf

3 Reserve Bank of India, "Annual Report 2023-24," *Government of India* (2024), https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/0ANNUALREPORT202324_FULLDF549205FA214F62A2441C5320D64A29.PDF

4 "India's UPI : A Global Front-runner in Digital Payment Systems," *Press Bureau of India,* October 30, 2023, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1973082&ref=indiatech.com.

5 Clause 10, DLG Guidelines dt September 02, 2022

6 Clause 7.4/Clause 7.5 PA Guidelines dt March 17, 2020

7 Kistenmacker, Yann. 2023. "Data Life Cycle Phases According To Google," *Medium*, October 7, 2023. https://medium.com/@yannkistenmacker_71035/data-life-cycle-phases-according-to-google-0f4fc3a130e1

8 Clause 10.2, DLG, September 02, 2022.

9 S. 38 (2) DPDP Act. *"In the event of any conflict between a provision of this Act and a provision of any other law for the time being in force, the provision of this Act shall prevail to the extent of such conflict."*

10 Clause 10.2, Guidelines on Digital Lending, dated September 02, 2022

"The borrower shall be provided with an option to give or deny consent for use of specific data, restrict disclosure to third parties, data retention, revoke consent already granted to collect personal data and if required, make the app delete/ forget the data."

11 Section 2(i), Digital Personal Data Protection Act, 2023 dated August 11, 2023.

12 Chapter V, Digital Personal Data Protection Act, 2023 dated August 11, 2023.

13 See Illustration to Clause 6(1), Digital Personal Data Protection Act, dated August 11, 2023

14 This is because in the absence of the specific inclusion of this category, REs/LSPs will have to rely on express consent under Section 4 or the general implied consent under Section 7 (a) that the data principal may only partly give (for instance, for credit underwriting) and partly deny (for example, for sharing of data with third party collection agents). Reading this along with the 'auto-expunging' illustration to Section 6(1) raises concern.

Key Takeaways

Amoha Basrur

As data breaches become an increasing concern, safeguarding financial data is paramount.[1,2] The Digital Personal Data Protection Act, 2023 addresses a critical gap in the regulatory framework, especially given the rapid evolution, involvement of non-traditional actors, and growing complexity of data ecosystems in the financial services sector. However, this sector, at present already highly regulated, faces the challenge of aligning the DPDP Act with existing regulations. Financial data is currently governed by a network of rules and regulations, including those issued by the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), and Insurance Regulatory and Development Authority of India (IRDAI).

The DPDP Act complements these sectoral regulations by providing more precise guidelines on data retention and deletion. However, certain prescriptive aspects of the Act, such as language requirements for consent screens and restrictive rules on data expunging, could hinder operations. Despite this, the Act defines responsibilities and rights across all stages of the data lifecycle, making it essential to align India's regulations with global standards, promoting trust, and fostering innovation.

Challenges, Implementation, and Impact

The DPDP Act outlines detailed requirements for data handling, including consent management, data retention, and deletion, which may pose challenges for fintech entities. Compliance will require significant investments in data processing, consent management, data storage, breach notification, and grievance redressal mechanisms. Entities operating on global platforms must also navigate the new requirements for cross-border transfers to ensure the continuity of data flows across jurisdictions.

Additionally, the Act imposes parallel obligations on different parties processing the same data, further complicating compliance efforts. Critics have argued that the Act is overly prescriptive in certain areas. For instance, the requirement to present consent screens in any of the 22 languages specified in the Eighth Schedule of the Constitution could complicate operations. Furthermore, the Act's provisions on auto-expunging data, where consent is no longer required, appear excessive from an industry perspective and extend beyond necessary data protection measures.

Concerns also arise from the apparent lack of understanding of the context surrounding certain services. The Act does not explicitly include provisions for 'enforcement and collection of debt'. This omission raises worries that borrowers may consent to data use for loan processing while denying data sharing with third-party debt collectors to whom debt collection—especially stressed debt—is usually outsourced. This situation could lead to a conservative credit approach that excludes certain borrowers from the market.

Similarly, although the Act aims to protect consumer data, overly stringent data protection measures might hinder the innovation necessary for fraud prevention services, which often require access to additional data. Additionally, greater clarity is needed on certain clauses, such as those related to algorithmic transparency. While algorithmic accountability is a vital issue, the broad phrasing of this clause allows excessive room for interpretation regarding the steps that companies must take to maintain transparency.

Regulators like the RBI, SEBI, and IRDAI must align their guidelines with the DPDP Act. Such alignment includes revising the 'know your customer' guidelines, data

retention policies, and customer data protection frameworks to prevent conflicts between current financial regulations and the principles of the DPDP Act.[3] Harmonising regulations also requires clarification on data retention and deletion to avoid disputes between the DPDP Act and other laws, such as the Prevention of Money Laundering Act.[4]

Given that financial institutions frequently outsource data processing activities to third-party vendors for tasks like credit scoring or fraud detection, specific requirements for third-party risk management are essential. These specifications should include data protection clauses in vendor contracts, audits of third-party data handling practices, and accountability mechanisms for data breaches involving third-party service providers.

Implementation Recommendations

1. **Implementation of Data Governance Framework:** Entities must develop a robust data governance framework that centres on the principles of 'privacy by design' and 'privacy by default' throughout all stages of the data lifecycle.
2. **Alignment of the Existing Regulatory Framework:** Regulators such as the RBI, SEBI, and IRDAI must align their guidelines and policies with the requirements of the DPDPA.
3. **Harmonisation of Regulations:** The Act should provide clearer guidelines to address potential overlaps between the DPDP Act and existing sectoral regulations. Corrective measures include issuing sector-specific guidelines and harmonised directives that define how entities should prioritise compliance when faced with conflicting requirements, particularly regarding data retention, deletion, and cross-border transfers.
4. **Promoting Awareness and Training:** Regulators must promote awareness of the Act's implications and how to comply with its requirements to ensure the cultural shift that the DPDP Act aims to create.
5. **Scenario-Specific Guidelines:** Clear guidelines are needed for specific data processing scenarios, such as debt collection and fraud detection. Regulators must periodically review the Act's impact to ensure it serves as a catalyst rather than a hurdle across various niches in the sector.
6. **Improved Coordination Among Regulatory Bodies:** Establishing structured coordination mechanisms between the Data Protection Board and sectoral regulators could help prevent conflicts and overlaps between financial regulations and data protection laws.

Conclusion

The DPDP Act emphasises individual consent, data minimisation, and secure data handling, representing a fundamental shift in India's approach to data protection. Its success will depend on the willingness of stakeholders to

prioritise data privacy. While the Act has garnered praise for its scope and vision, upcoming regulations must address its interaction with existing frameworks, fill gaps in sector-specific regulations—such as stringent data localisation requirements—mitigate compliance costs for financial institutions, and clarify ambiguity surrounding cross-border data flows. The effective implementation of the DPDPA in the finance sector will require clear guidelines and ongoing dialogue with stakeholders to ensure that regulations consider the unique contexts and challenges within financial services, ultimately fostering a competitive digital economy in India.

Amoha Basrur is Junior Fellow, Centre for Security, Strategy and Technology, Observer Research Foundation.

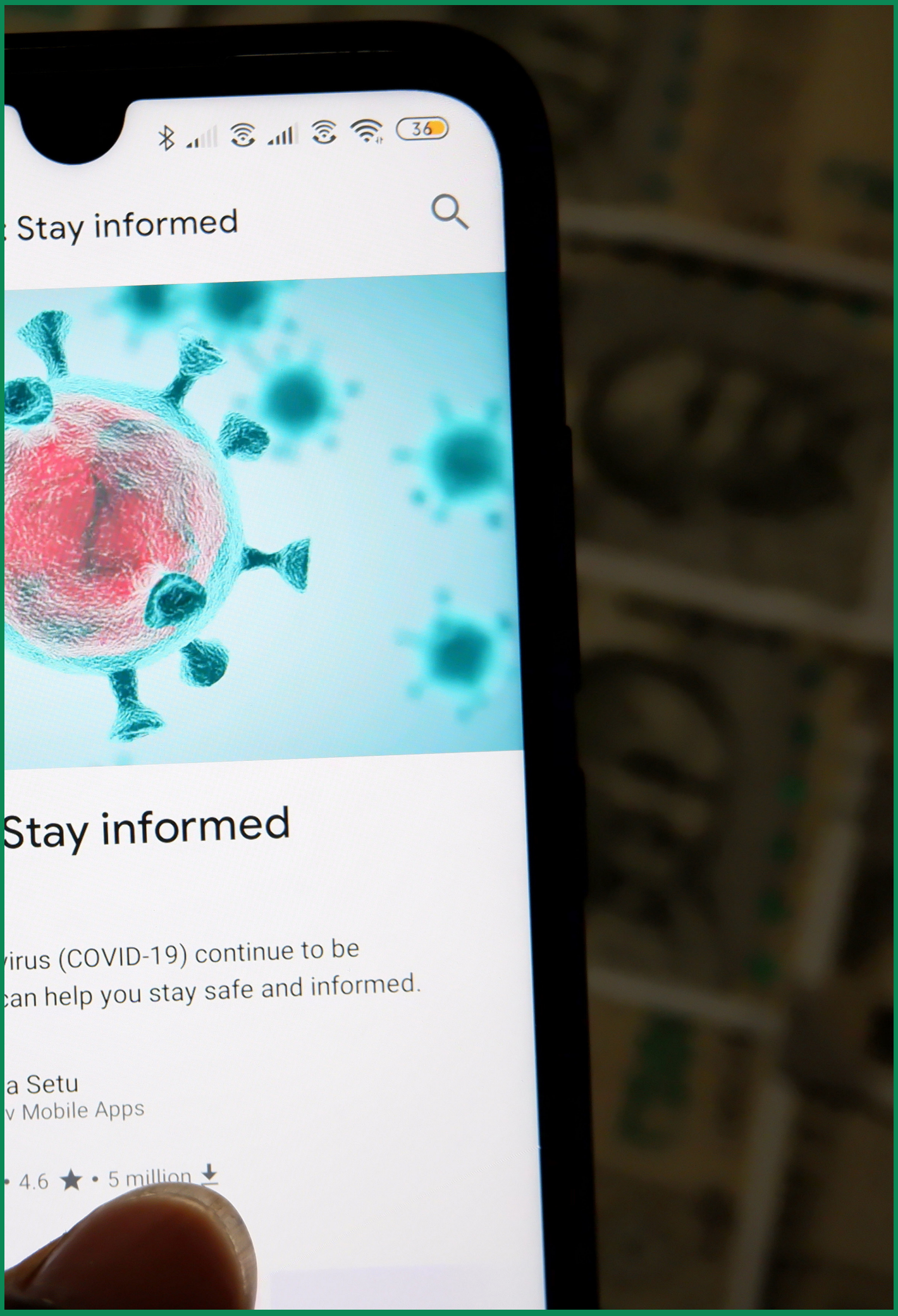
Endnotes

1 Vidhi Taparia, "Avg Data Breach Cost in India Rises 28% in 3 Years," *Fortune India,* July 30, 2024, https://www.fortuneindia.com/macro/avg-data-breach-cost-in-india-rises-28-in-3-years/117812.

2 "India's Financial Data at Risk: 17% Store Passwords Unsafely, 53% Face Fraud," *Business Today,* July 2, 2024, https://www.businesstoday.in/technology/news/story/indias-financial-data-at-risk-17-store-passwords-unsafely-53-face-fraud-435385-2024-07-02.

3 Deepankar Sanwalka et al., *Implications of the DPDP Act 2023 on India's Financial Services Sector, Implications of the DPDP Act 2023 on India's Financial Services Sector,* Grant Thorton Bharat, 2023, https://www.iamai.in/sites/default/files/research/Implications%20of%20Digital%20Personal%20Data%20Protection%20Act%202023%20on%20India%26%23039%3Bs%20Financial%20Services%20Sector%20-%20Unveilled%20at%20GFF%20202%20%281%29_compressed.pdf.

4 "How Will the DPDP Act Impact Financial Services?," Grant Thornton Bharat, https://www.grantthornton.in/insights/articles/how-will-the-dpdp-act-impact-financial-services/.


Stay informed
Stay informed
irus (COVID-19) continue to be
an help you stay safe and informed.
a Setu
v Mobile Apps
• 4.6 ★ • 5 million

03

HEALTH DATA

Academic Perspective

Astha Kapoor

An Application Perspective

Anurag Verma

Key Takeaways

Vaishnavi Sharma

Academic Perspective

Astha Kapoor

India has faced healthcare and infrastructure challenges for long, and the COVID-19 pandemic has only exacerbated the difficulties. In recent years, more attention has been given to the role of health data in driving solutions such as personalised medical services and more insightful public health research. The increasing generation of health data, along with a shift toward digitisation—driven by private sector initiatives in telemedicine[1] and e-pharmacy,[2] and the push for technological standards for electronic health records[3]—highlights the importance of access to health data. However, such access must be balanced with the need to protect the data, given their unique sensitivity and the privacy risks associated with misuse.

A historical set of sectoral rules and policies, such as the Electronic Health Record Standards for India, currently govern health data in the country. These standards establish principles for privacy and the handling of data points categorised as 'protected health information' and 'personal health data or information',[4] which include information like health risk and status. Other directions impacting health data include the 'National Ethical Guidelines for Biomedical and Health Research Involving Human Participants,'[5] issued by the Indian Council for Medical Research (ICMR), which addresses data collection, management, ownership, individual consent, and privacy. In 2021, the ICMR also released guidelines for 'Good Clinical Laboratory Practices',[6] which cover data security.

Additionally, the national telemedicine service eSanjeevini's 'Telemedicine Practice Guidelines,' issued by the Ministry of Health, focuses on patient records, diagnostic data, and images.[7] The Sensitive Personal Data and Information Rules, 2011 under the Information Technology Act provide a core framework for health data regulation in the absence of a specific data protection law. Other relevant regulations include the Clinical Establishments (Registration and Regulation) Act and ancillary regulations like the Telecom Commercial Communication Customer Guidelines of 2010, which impact health data processing.

Further efforts to create a cohesive health data management framework, such as the Digital Information Security in Healthcare Act (DISHA), which focused on patient data and setting up a Health Information Exchange for data storage and transmission, have been set aside in favour of a general data protection law to regulate personal data processing and safeguard individuals' privacy.

Earlier drafts of such a law (such as the Personal Data Protection Draft)[8] specifically defined 'health data' as "data related to the state of physical or mental health of the data principal and including records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, or data associating the data principal to the provision of specific health services," and appropriately categorised it as sensitive personal data. These drafts have now been formalised as the Digital Personal Data Protection Act, 2023.

The DPDP Act, however, does not create a separate category for health data or sensitive personal data, nor does it explicitly state that health data is a sub-category of personal data. As a result, the protection and use of health data remains open to interpretation. In many jurisdictions, health data is treated as a separate category to provide it with the necessary oversight due to its sensitivity. In India, it remains to be seen whether the DPDP Act will suffice or if a specific framework for health data will be required.

Practices in Other Jurisdictions

India's health ecosystem can be improved through digital health solutions

whose designs consider the country's complexities and unique challenges. Democratising access to quality preventive and palliative care, along with health insurance mechanisms, remains a critical challenge—one the private sector is increasingly stepping up to address. In areas where access to physical healthcare infrastructure is limited, telemedicine can serve as a valuable first touchpoint for patients. However, issues like the digital divide and lack of awareness mean that 80 percent of India's population remain underserved by digital health solutions. Telemedicine, for example, primarily reaches only the wealthiest 20-30 percent of the population, with most services concentrated in the metropolitan areas.[9] Beyond these challenges, private digital healthcare actors also face security and regulatory concerns. A patchwork of policies, guidelines, and laws govern the collection and use of health data.

While data protection legislation may not be able to resolve infrastructural and awareness issues, they could be useful in filling the gaps in privacy and security. The need for stronger security measures and effective responses to breaches is evident, especially given the significant cyberattacks in recent years; the United Nations has called attention to the increasing incidence of cyberattacks on healthcare systems.[10] Globally, health data breaches carry strict liability for incidents like those experienced by AIIMS, where a ransomware attack compromised the entire digital system of India's biggest hospital.

In the United States (US), the Health Insurance Portability and Accountability Act (HIPAA) classifies a ransomware attack as a security incident, and covered entities are required to implement an incident response plan to identify, respond to, and mitigate the impact of such attacks.[11] Similarly, the UK's Information Commissioner's Office takes a strong stance on health data breaches, recognising the sensitivities involved.[12] In Australia, and across the EU, the GDPR treats health data as a separate category, offering robust safeguards to protect it and foster innovation in delivering better healthcare.[13] The UAE too, has a separate health data protection law that takes a strong stance on security and breaches.[14] Building trust in digital healthcare systems through clear regulations and security rules is crucial to increasing usage by service providers. Both individuals and businesses in the health sector would benefit from a clear and harmonised policy framework for the protection and use of health data, as seen in other jurisdictions.

Challenges

The DPDP Act has brought data protection into sharp focus in India, and the upcoming notification of its rules will clarify the implementation of this long-awaited legislation. However, it is important to recognise that the Indian healthcare ecosystem is vast, comprising numerous private and public entities such as hospitals, clinics, laboratories, pharmacies, and insurance providers. Despite efforts to digitise the ecosystem, a significant portion of India's health infrastructure remains offline, making it a complex sector to implement

comprehensive data protection measures. Even where digital infrastructure exists, challenges may arise in implementing the DPDP Act in the health sector. Most notably, the legislation does not specifically address health data, thus overlooking its sensitive nature and the oversight it requires. It also fails to address nuances such as 'social data'—data collected from non-traditional sources like social media and health tracking applications,[15] which are increasingly used for health purposes. This gap highlights the regulation's inability to fully address the complexities of health data processing as technology evolves. The DPDP Act also lacks a definition of harms, which is critical in the context of health data. Potential harms include economic impacts (such as overpaying for insurance or job loss), physical harm, and psychological effects, which differ from the harms associated with other types of data misuse.[16] The DPDP Act's regulatory authority, the Data Protection Board (DPB), must establish clear guidelines for handling sensitive data, as distinct from other data types. Moreover, it is crucial to understand how sectoral efforts like the Health Management Policy, Unified Health Interface in the Ayushman Bharat Digital Mission, will interface with the DPDP Act, especially since they all focus on private sector oversight of health-service delivery. The industry also needs reassurance that it will not have to seek approvals from multiple regulatory bodies for health data processing and use. It must be clarified whether governance will come from the DPB or the Ministry of Health and Family Welfare, which is the presumed touchpoint for the health sector. The overlap in compliance with various regulations, combined with the need for approvals from different regulatory bodies, can lead to inefficiencies and confusion. Harmonising these frameworks is essential for effective implementation.

Implementing specific clauses of the DPDP Act for health data requires careful consideration, as there are grey areas that need to be addressed. For example, Section 6 (4) of the DPDP Act gives the data principal the right to withdraw consent, and the data fiduciary is required to stop processing the data, except in certain cases. In the health sector, medical histories are vital for providing ongoing care, and it is unclear how this provision will align with the practical needs of healthcare services. Additionally, there is a need to clearly define what constitutes a 'lawful purpose' for processing health data, as the risk of misuse is high in this sensitive domain.

The current DPDP Act framework, by not clearly defining sensitive data, falls short in addressing the security and privacy issues specific to health data. There is a pressing need to develop security guidelines that bring to life the principles of anonymisation and purpose limitation outlined in the DPDP Act, with a particular focus on health. These guidelines should incorporate lessons from regulations like HIPAA and others to establish clear, effective safeguards for personal health data.[17]

The DPDP Act introduces consent managers—i.e., a consent layer to move data from data provides (e.g. hospitals) to data users (e.g. doctors)—which will play a crucial role in managing health

data, as outlined in the ABDM's Health Stack document.[18] It is essential to test the function of health consent managers and understand how they may differ in form and function from those in the financial services sector. This presents a valuable opportunity for regulatory and private sector innovation to collaborate.

Finally, as noted earlier, the health sector is one of the least digitised spaces in India. Any effective digital data protection legislation must consider that a significant amount of data is still not digital and ensure that patient privacy is protected throughout the system.

Beyond sector-specific issues, there are common concerns with the DPDP Act, which puts the burden of sectoral applications of the act on the industry. There is a need to reduce space for interpretation, through the overall rules for implementation. There is ambiguity in the industry regarding the roles and compliance requirements of data fiduciaries and data processors, which need clarification so entities can self-identify and establish strong contractual agreements.[19] It is also essential to create a category for companies that act as both data fiduciaries and data processors to ensure clarity of roles and responsibilities. Additionally, sectoral regulators must clarify the boundaries and obligations in these roles.

The current data protection framework is high-level and open-ended. Therefore, ensuring the regulatory authority and independence of the DPB is critical. The board must have adequate resources and authority to implement this multifaceted regulation, including investigating security breaches and related harms. Furthermore, the board's role must be clearly defined in relation to sectoral regulators like TRAI (telecom) and the National Health Authority (health), as well as subject-matter regulators like the Competition Commission of India, all of which deal with data-related issues. Lastly, the role of the board in grievance redressal for individuals needs to be carefully designed and implemented to establish and maintain trust in the regulator, both among complainants and the broader ecosystem, which must witness the regulator's unbiased and authoritative nature.

Another overarching issue that the DPB must consider is the delicate balance between regulation and innovation. In the health sector, the start-up ecosystem plays a vital role in meeting last-mile demands, and therefore creating an environment conducive to fostering sustainable solutions is crucial. One potential approach is the adoption of a sandbox model which can provide a controlled environment to test new technologies, data management strategies and regulatory approaches for health data. Sandboxes have been successfully employed in the financial services sector, and could offer significant value in healthcare as well.

All these challenges highlight the gaps in protecting individual rights within the health sector under the DPDP Act. Key

rights, such as the right to be forgotten and the right to data portability, are absent. Additionally, there are potential harms to privacy rights stemming from the ambiguity around the 'legitimate use' of data which maybe be exploited for legitimate uses such as disease surveillance but compromise the privacy of individuals. Further, the framework does not acknowledge collective data rights or group rights, which acknowledge the relational nature of data, and puts the onus of safeguarding data not on individuals who are likely powerless but empower groups to steward group data, critical in the context of health data.[20] One potentially interesting inclusion in the DPDP Act is the right to nominate, offering users control over their data after death, though this right too, could be vulnerable to exploitation.

The Way Forward

The implementation of the DPDP Act in the health sector will not be straightforward, particularly given the complexities and sectoral variations in healthcare. In this context, regulation needs to be tiered to account for the realities of the diverse actors within the healthcare ecosystem. A granular approach should differentiate between the following:

1. Small clinics and healthcare providers
2. Medium-sized clinics, which might need data protection officers for compliance
3. Large hospitals and health networks, which will require data protection impact assessments and clear communication of data-processing activities
4. Health tech companies processing large-scale data for products and services, necessitating higher levels of compliance
5. Big tech companies involved in health data processing

In this context, the DPB will need to collaborate closely with the Ministry of Health and Family Welfare to coordinate a cohesive approach to data governance in healthcare. This approach should be meaningful to health service providers, innovators, and citizens—whose well-being remains central to the data governance discourse.

In broader terms, for the DPDP Act to be successful not only in the health sector but across industries, it is crucial to build capacity and raise awareness, particularly among smaller players who may face a compliance burden and lack the resources to fully understand and implement the legislation's provisions. The DPDP Act is only a starting point, and there will be a continuous need to monitor its implementation, identify where entities are struggling to comply, and recognise areas where the framework may be insufficient and requires further developments. Maintaining constant engagement between the DPB and various stakeholders will be vital in understanding experiences with the DPDP Act and fostering an environment that allows for evolution and innovation in data protection.

Conclusion

The DPDP Act is a welcome and necessary development, particularly given the prolonged wait for a cohesive data protection framework in India—a country at the forefront of digital inclusion and access. The current iteration of the legislation, however, is diluted, leading to some of the concerns highlighted earlier in this article. For the health sector specifically, it is critical to recognise the unique nature of health data, given its sensitivity and immense value to both individuals and the industry. Additionally, the vast and varied landscape of the health sector—ranging from entirely offline providers to highly data-driven health technologies—demands a unified and cohesive data governance strategy. This strategy must not only translate the DPDP Act into actionable sectoral guidelines but also address the fragmentation in the health data policies, regulations, and guidelines currently in place. Such an approach is vital to ensuring clear communication with different players in the private healthcare sector regarding compliance, and to enabling citizens and patients to build and exercise trust in health data governance processes.

Astha Kapoor is Co-Founder, Aapti Institute.

Endnotes

1 Deloitte, "Is the Telemedicine Boom Over?," https://www2.deloitte.com/in/en/pages/life-sciences-and-healthcare/articles/is-the-telemedicine-boom-over.html.

2 S. Agarwal et al., "Telemedicine During the COVID-19 Pandemic," *Journal of Family Medicine and Primary Care* 11, no. 2 (2023): 313–319, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9804119/.

3 National Resource Centre for EHR Standards, "EHR Standards for India," https://www.nrces.in/standards/ehr-standards-for-india#intro

4 "EHR Standards for India"

5 Indian Council of Medical Research, "National Ethical Guidelines for Biomedical And Health Research Involving Human Participants," https://ethics.ncdirindia.org/asset/pdf/ICMR_National_Ethical_Guidelines.pdf.

6 Indian Council of Medical Research, *Good Clinical Laboratory Practices (GCLP) Guidelines*, 2020, https://main.icmr.nic.in/sites/default/files/guidelines/GCLP_Guidelines_2020_Final.pdf.

7 Ministry of Health and Family Welfare, Government of India, *Telemedicine Practice Guidelines* (India: Ministry of Health and Family Welfare, 2020) https://esanjeevani.mohfw.gov.in/assets/guidelines/Tele.

8 Ministry of Electronics and Information Technology, Government of India, *Data Protection Framework* (India: Ministry of Electronics and Information Technology) https://www.meity.gov.in/data-protection-framework.

9 "India's Healthtech Sector Growing Faster Than Global Peers, But There's a Catch," *NDTV Profit*, https://www.ndtvprofit.com/amp/economy-finance/indias-healthtech-sector-growing-faster-than-global-peers-but-theres-a-catch.

10 "Cyberattacks Also Extended Beyond Hospitals to Include Clinical Trial Software Vendors and Laboratories," *United Nations News*, November 2024, https://news.un.org/en/story/2024/11/1156751#:~:text=Cyberattacks%20also%20extended%20beyond%20hospitals,trial%20software%20vendors%2C%20and%20laboratories.

11 U.S. Department of Health and Human Services, "Ransomware Fact Sheet," Health Information Privacy, https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html.

12 NHS England, "Personal Data Breaches," Transforming Health and Care https://transform.england.nhs.uk/information-governance/guidance/personal-data-breaches/.

13 European Data Protection Supervisor, "Health," https://www.edps.europa.eu/data-protection/our-work/subjects/health_en#:~:text=The%20General%20Data%20Protection%20Regulation,data%20for%20data%20protection%20purposes.

14 PwC, *Healthcare Data Protection in the UAE*, https://www.pwc.com/m1/en/publications/healthcare-data-protection-in-the-uae.html.

15 "Assessing Social Data as Real-World Data: Its Benefits, Its Risks, Its Future," *Vox.bio News,* https://vox.bio/news/assessing-social-data-as-real-world-data-its-benefits-its-risks-its-future/.

16 L.O. Gostin et al., "Health Privacy During the COVID-19 Pandemic," *Journal of Health Affairs* 39, no. 5 (2023): 871–878, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9610324/#:~:text=Health%20Privacy%20during%20the%20COVID,swung%20to%20contain%20the%20pandemic.

17 Shravishtha Ajaykumar et al., *Digital Personal Data Protection Act 2023: Recommendation for Inclusion in the Digital India Act,* New Delhi, Observer Research Foundation, 2023, https://www.orfonline.org/wp-content/uploads/2023/10/ORF_SpecialReport_DigitalPersonalDataProtectionAct2023.pdf

18 National Health Authority, Government of India, *National Health Stack Strategy and Approach*, (New Delhi: National Health Authority, 2018), https://abdm.gov.in:8081/uploads/NHS_Strategy_and_Approach_1_89e2dd8f87.pdf

19 "Distinguishing Between Data Fiduciaries and Data Processors: Insights from PrivacyNama 2023," *Medianama*, https://www.medianama.com/2023/11/223-distinguish-data-fiduciary-data-processor-privacynama/

20 Linnet Taylor, Luciano Floridi, Bart Van der Sloot, eds., *Cybersecurity for Digital Transformation: A Comprehensive Guide*, https://link.springer.com/book/10.1007/978-3-319-46608-8.

An Application Perspective

Anurag Verma

Healthcare—comprising hospitals, medical devices, clinical trials, telemedicine, medical tourism, health insurance, and medical equipment—has become one of India's largest sectors, both in terms of revenue and employment. The strengthening of coverage, expansion of services, and increase in expenditure by public as well as private players have driven its growth in the recent years.

In this context, data will become only more important in managing the health sector. Healthcare providers, notably large private hospitals and diagnostic laboratory chains, collect a patient's personal data in digital form, whether through software like those used for filing the electronic health record (EHR) and electronic medical record of a patient, scheduling appointments, providing medical diagnosis and electronic prescriptions, or offering

telemedicine service.[1] Today, there are more than 10,000 healthcare start-ups[2] providing various health-related services, including telemedicine platforms, digital health monitoring services, EHR systems, AI-driven diagnostics, and e-pharmacy facilities. They collect various health-related data through wearable devices, mobile applications, or medical devices that are now essentially digital in nature. In addition, government schemes such as the 'Digital India' programme have brought tremendous changes in the country's healthcare sector.

Initiatives like the Ayushman Bharat Digital Mission (ABDM), the Central Government's initiative for building a digital health ecosystem, and Aarogya Setu—an app to connect essential health services with the people in its fight against COVID-19, and now transformed into a national health app offering digital health services—have made healthcare facilities and services more accessible to larger populations of the country.

However, in the absence of any existing privacy regulations and rules on how to handle the data thus generated, practices are not uniform. From the patient's perspective, there is a lack of clarity on the purpose of collection of their data, how it is processed, whether there are data protection mechanisms in place, and how data is shared with third parties. While some large healthcare providers may follow certain best practices based on global industry standards, this is not implemented across the board and current digital data collection methods and privacy principles are vendor-specific.

Organisations that operate in countries where privacy regulations are already in place—such as Europe with the General Data Protection Regulation (GDPR),[3] or the US's Health Insurance Portability and Accountability Act (HIPAA)[4]—may have some level of compliance to those underlying privacy principles when operating in India. For healthcare providers that operate only in the Indian region, however, even partial compliance to such standards is not mandated. This gap needs to be addressed. In this context, the Digital Personal Data Protection Act, 2023[5] becomes highly relevant.

Industry Standards and Expectations

Global best practices, like those outlined in GDPR and HIPAA, emphasise data minimisation, transparency, and purpose limitation. Indian healthcare providers are now expected to adopt similar principles, including secure data handling, clear consent mechanisms, and accountability for data sharing. The DPDP Act introduces compliance obligations for healthcare entities, fostering a culture of privacy-first healthcare services that safeguard patient data while supporting India's fast-growing digital health ecosystem.

As healthcare organisations navigate data protection compliance, understanding the full scope of their data lifecycle is essential. Companies typically begin their data protection compliance journeys by conducting an inventory of the data they collect and classifying it into personal data, sensitive personal data and non-personal data. While this classification

is not strictly necessary for DPDP Act, it is still a useful exercise to carry out and can give useful insights on the likelihood of a company's classification as a significant data fiduciary (SDF). SDFs also need to carry out data protection impact assessments, and this inventory and classification of data is an important part of these exercises.

Data Lifecycle

The data lifecycle refers to the stages through which data flows—i.e., collection, storage, processing, sharing, and deletion. It is crucial for healthcare providers to manage each phase. It is a continuous, policy-based process where each phase informs the next, and consists of the following stages:

Collection: The first stage in the data lifecycle is collecting personal data from various internal and external sources. From the healthcare perspective, one needs to prioritise collection of data through direct interaction with the patient. For instance, the first interaction of the patient when visiting the healthcare provider is registration. As part of this, the patient's personal details, along with existing medical history, must be collected. As per the DPDP Act, the collection must be done in a transparent manner with the informed consent of the patient who has had access to a privacy notice made available on the company's website.

Storage: Once data is collected, it needs to be stored. Rather than scattering data across different department or tools, it is preferable to store it in a centralised repository, so that it can help in meeting compliance requirements, especially when a data subject's request needs to be processed.[6]

Processing: Data processing involves data sanitation, anonymisation, encryption (of either the database or storage) and compression of any large medical data like medical imaging data. From the DPDP Act's perspective, correct data processing will ensure compliance with data protection regulations and minimise the impact of any data breaches.[7]

Analysis: Data analysis involves studying processed or raw data to identify trends and patterns through machine learning, AI, or any other computer algorithms. This stage is critical as it provides valuable insight—the cancer risk score for a cancer-screening product, for instance, can help in providing a better level of care.

Deployment: This is when data sharing and usage happens. For instance, when a medical report is generated, it is then shared with relevant stakeholders—generally, doctors and the patient. The intended use and sharing should be clearly indicated at the time of taking patient consent.

Archiving: Data that is no longer actively used is archived. This ensures that historical data is preserved for future reference or compliance purposes (such as in the event of a medico-legal case). However, data should only be kept for a defined period to reduce data-breach

risks. If no longer required or the patient requests it to be removed, data should be deleted.[8] The privacy notice shared with the patient should cover the organisation's data retention policy.

Data Life Cycle Illustration

Let us examine the data lifecycle with a hypothetical scenario. X, a patient, wants to avail a breast cancer screening with the healthcare provider Y. X will visit the clinic where this service is being offered. Y's technician will need to collect X's personal data and complaints history, and capture a thermal image of the breast region. Before collecting this information, Y needs to provide a consent form and privacy notice to X. Once X has given consent, Y will collect the required data and thermal breast images of X. The data collected will be validated and stored in the database. At the processing stage, thermal images will be compressed (if required) and encrypted before being stored. The next stage will be analysis, where the patient's thermal images will undergo analysis using AI/ML. The analysed image will again be encrypted before it is stored.

Thereafter, in the deployment stage, a medical report will be generated based on the analysis and this will be shared with the doctor for review. Once the doctor has reviewed and approved the report, it will be shared with X via email. After a couple of months, the collected data and analysed images will be archived as per the retention period or when the patient sends a request to Y to delete the data.

Global Industry Standards for Data Protection Vs. the DPDP Act

The following paragraphs summarise the key differences between the GDPR and the DPDP Act:

Grounds for processing: The DPDP Act allows for the processing of personal data for certain 'legitimate uses.'[9] This is not the same as the wider 'legitimate interests' ground that the GDPR provides.[10] This implies that Indian law is consent-centric and will require businesses to collect explicit consent for many processing activities, which could add to the compliance cost.

Public data: The DPDP Act takes 'publicly available' personal data entirely out of the scope of the legislation.[11] As an example, if an individual, while blogging her views, has publicly made available her personal data on social media, then processing of that data will no longer come under the purview of the data protection law. This contrasts with the GDPR where, irrespective of where personal data is sourced from or is otherwise available, the obligations of the law continue to apply. The Indian law is also not clear as to what constitutes 'publicly available' data. This is important for healthcare AI companies that largely rely on publicly available health datasets to train their models.

Significant data fiduciaries (SDFs): Unlike the GDPR, the DPDP Act creates a category of SDFs[12] that are subjected to higher obligations, like the appointment of a data protection officer,[13] the mandate

to conduct a data protection impact assessment,[14] and an independent data audit.[15] It may not exempt start-ups if they fall under the category. This could pose hurdles for businesses, especially those focused heavily on growth.

Cross-border data transfer: Under the DPDP Act, data transfer is permitted to jurisdictions outside of India other than those blacklisted by the Indian government. The law does not mention the criteria for notification of countries under the blacklist.

Data breaches: Unlike the risk-based approach of the GDPR, the DPDP Act mandates that a data breach is reported regardless of the magnitude or risk of harm. This in addition to an existing mandate to report data breaches and other specified cyber incidents to the Indian Computer Emergency Response Team (CERT-In).[16] This implies that data fiduciaries will have to file at least two reports for each data breach.

Data retention periods: The GDPR requires that entities retain data only until it is necessary for the purposes for which it was collected, but does not prescribe a retention period. This gives a degree of flexibility to the data-processing entity to determine the retention period for the data it collects. The DPDP Act follows a similar standard, but with a more prescriptive approach to deciding when a purpose is served.[17] The DPDP Act thus provides far less flexibility to a data fiduciary in terms of determining data retention periods.

Requirements of the DPDP Act Implementation Process

Data inventory and mapping: Though the legislation does not mention this explicitly, SDFs will be required to create a comprehensive inventory of personal data and map how data flows within the organisation—from origin to its various destination and uses. As data will most likely be spread across different departments (human resources, finance, operations, engineering), each department owner should be consulted in this inventory exercise. In accordance with the data lifecycle, SDFs should capture various data collection sources (emails, apps, patient visits), where data is stored (primary/secondary storage locations), data-processing activities, with whom the data is shared internally and externally, and the data-retention duration. If the data is stored on a third-party platform (whether through an on-premise or cloud-service provider, or a software-as-a-service provider), then this should also be mapped. Data inventory and mapping will be an ongoing process.

Consent mechanisms: Data fiduciaries must implement clear and specific (instead of blanket) approvals and adopt an informed consent process[18] that is available in different regional languages. Websites utilise various categories of cookies for different purposes, such as personalising user experience, load balancing, and targeted advertising. Because of the legal constraints, businesses must obtain user consent before deploying non-essential cookies on devices. Websites collecting any personal

data (via cookie) must display a cookie consent banner to first-time visitors, and give users the choice to opt out of non-essential cookies.

Privacy notice: A privacy notice must be available at the time of availing services. This can be published on the company website or apps and should capture what all personal data is collected, data sources, purpose, any data sharing, including with third parties, and mention all an individual's rights with respect to the viewing, modifying, or deleting of their data. It must also include the organisation's full contact information with its name and address and the email of the privacy officer.

Training at the organisation level: Once the data mapping is carried out, relevant stakeholders dealing with personal data must be identified and provided training on the DPDP Act regulations. This training can be customised based on role and responsibilities. Effectiveness checks should be conducted, such as in the form of a quiz.

Privacy incident management:[19] Policies and procedures must be in place for incident management. These should capture the mechanism by which anyone within the organisation can report a privacy incident using a privacy incident form that is accessible from wherever the employee is working. A case study-based approach can be adopted as part of the training, wherein a sample case study related to a privacy breach needs to be reported can be given. Privacy officers can evaluate the incident response and provide feedback related to the accuracy of the filing.

Documentation and compliance: A comprehensive compliance checklist and documentation of compliance must be maintained. Key metrics, like the number of privacy incidents that have happened vs the number that have been reported, and the number of data subject requests processed, must be captured. These can be presented in management review meetings where top management and data owners are present. This will be useful when independent audit is being conducted.

Third-party contracts: All contracts for vendors handling personal data must be reviewed.[20] Contracts must have a privacy clause mentioning the purpose of data collection, data protection mechanisms in place, mandates regarding sharing of data externally, and reporting any data privacy breach to the data fiduciary.

Appointment of a data protection officer: SDFs must appoint a data protection officer well-versed with privacy regulations.

Challenges to DPDP Act Implementation

Behavioural changes and added training requirements: Making the move to an organisational culture that prioritises data privacy can be difficult. Employees need to understand and embrace the importance of DPDP Act compliance. This requires regular training and awareness programmes to ensure that employees understand DPDP Act requirements and

follow compliant practices. In addition, in healthcare, frontline workers like technicians and nurses require specific training tailored to their work.

Gap assessment and data mapping: Implementing the DPDP Act requires conducting an initial audit of existing systems to assess compliance. This necessitates creating a comprehensive inventory of all personal data and mapping its flow within the organisation, which is complex and time consuming, given that data can come from different platforms like apps, websites, and third parties. Moreover, each department within an organisation collects and stores data differently. Mapping data thus becomes a massive task.

Security controls: Any personal data breach,[21] irrespective of the risk, must be reported under the DPDP Act. This strict requirement means stringent security controls must be in place to protect data. Implementing and maintaining strong security measures to protect personal data from breaches is an ongoing challenge.

Compliance with multiple privacy regulations: For organisations working across different geographic locations, the DPDP Act adds the burden of another regulatory compliance. The differences between it and other global regulations (GDPR, HIPAA) must now be taken into consideration.

Increase in costs: While large healthcare providers will be able to allocate additional budget, start-ups and small- and medium-sized enterprises with limited budgets will face challenges. They will most likely need to hire the services of companies that specialise in privacy law, thereby increasing their costs. Conducting independent audits will also add to the cost.

Consent management: Most consent forms are written in excessively legal jargon; this must be changed for the general user. Support for different regional languages must be added.[22] Given the different levels of education of Indian patients, understanding consent and giving it can pose additional challenges. Furthermore, for data fiduciaries with large customer bases, consent requirements will need changes in their existing operations. Documenting and maintaining user consent records[23] is important to demonstrate compliance, which adds to the record management overhead.

Rights of data principals: Implementing processes to handle data principal requests, such as access, correction, and deletion of personal data[24] requires robust systems and procedures. Managing these requests efficiently can be demanding if the volumes are high.

Data retention: Keeping track of when to delete data once it has reached the data retention limit[25] is going to be cumbersome, especially if data is spread across different storage and databases.

Potential Impact of the DPDP Act

The DPDP Act introduces numerous requirements to enhance data processing

accountability. Effective compliance with these new rules will have significant impact on the way organisations are run.

Data protection impact assessments (DPIA): Indian healthcare providers that collect significant volumes and sensitive personal data of patients will most likely fall under the category of SDFs. These SDFs will have additional obligations, including the appointment of an independent auditor and undertaking DPIA. The assessment is an exhaustive questionnaire to understand the potential risk and impact of any new project (for example, a new clinical trial) where personal data collection is involved. Organisations must assess potential risks to individuals' rights and implement necessary mitigations, which is the main purpose of this exercise. This is a time-consuming process and requires proper diligence.

Rethinking budget planning: Allocating resources for compliance with the DPDP Act will require careful budgeting. The impact to start-ups with tight budgets will be significant.

Balancing privacy and innovation: Organisations must strike a balance between innovative data-driven solutions and ensuring compliance with privacy principles.

Vendor management: Organisations often rely on third-party vendors for services. They will now need to ensure that these vendors also comply with DPDP Act requirements. This will require assessing their vendors' data handling practices and establishing contractual agreements that align with the legislation.

Changing regulations: DPDP Act compliance is going to be an ongoing process, and organisations will need to be up-to-date with regulatory changes and adapt their practices accordingly.

Areas for Improvement

Given the challenges and impacts highlighted in the previous sections, the following measures will help ease compliance.

Phase-wise implementation: The DPDP Act is quite comprehensive. It is suggested that phase-wise implementation milestones with flexible timelines be provided. The sections of the legislation that can be met with minimal implementation effort can be part of the first phase; sections with increasing level of implementation efforts can be added in subsequent ones.

Clear guidelines: Government should provide clear implementation guidelines and resources to navigate compliance effectively. This is quite similar to the resources that have been setup for GDPR and HIPAA compliance.

Special provisions for start-ups and SMEs: For start-ups and SMEs, the focus is on innovation and growth. The Act could provide more detailed guidelines on its applicability to them to ensure they are not disproportionately burdened. Striking the right balance between protecting personal data and fostering innovation is crucial. Overly stringent regulations could stifle technological advancements and economic growth.

Incident management: More specific requirements for incident management and breach notification processes would help organisations respond more effectively to data breaches. In addition, it should cover breach only of significant risk rather than reporting every breaches.

Delayed enforcement of penalties: It will take time to achieve full compliance, and any penalty should be made effective three years post the date on which the legislation comes into effect.

Public awareness and workshops: Awareness campaigns to educate the public about their rights must be promoted. Workshops must be conducted for industries to ensure effective implementation. This can be done on similar lines as to what has been done for ABDM.

Knowledge sharing: Knowledge sharing on implementation within healthcare verticals will help stakeholders learn from each other. Any course correction can be done early in the implementation cycle.

Conclusion

With the increasing trend towards digitisation of health data, the DPDP Act has been enacted at a crucial time to help fulfil goals of data privacy and protection. It provides a comprehensive framework and is on par with other data privacy regulations in the world, while incorporating requirements unique to the Indian context.

It will empower patients to have better control of their data. This shift to patient-centric data practices is a significant step. This will build trust in digital health services and increase usage of digital platforms. This will require healthcare providers to adapt the current business practices. While this will impose challenges for them, it will provide better data governance and enhance their reputation for data protection.

The effectiveness of the DPDP Act will be dependent on its implementation and enforcement. Government support in terms of clear guidelines, workshops, and resources especially for start-ups will be critical for implementation. The Act should be continuously reviewed and updated to keep up with technological innovations and address practical implementation challenges.

Overall, the DPDP Act represents an advancement in India's data protection landscape. Its success will depend on effective implementation, continuous adaptation to technological advancements, and active participation from all stakeholders.

Anurag Verma is a fractional CTO to healthcare startups, He has served as Head of Engineering, CISO and Privacy Officer at NIRAMAI.

Endnotes

1 Tosif Saiyad, "Top 10 Hospital Management Software Solutions in India," Bigscal - Software Development Company, October 24, 2024, https://www.bigscal.com/blogs/healthcare-industry/top-10-hospital-management-software-in-india/.

2 Tracxn, "HealthTech sector in India Overview," https://tracxn.com/d/explore/healthtech-startups-in-india/__MutePgNynK-p_w7M5fCLi6PdHq4hFSDFEA0QmrNLscA#Key-statistics

3 General Data Protection Regulations, "Legal Text," April 22, 2024, https://gdpr-info.eu/.

4 Office for Civil Rights, "HIPAA Home," April 19, 2024, https://www.hhs.gov/hipaa/index.html.

5 Ministry of Electronics and Information Technology, Government of India, "Digital Personal Data Protection Act, 2023," https://www.meity.gov.in/content/digital-personal-data-protection-act-2023.

6 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-Section 12(1)," 2023.

7 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-Section 33," 2023.

8 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-Section 12," 2023.

9 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act -Section 7,"2023.

10 General Data Protection Regulation, "Article 6-Lawfulness of Processing," https://gdpr-info.eu/art-6-gdpr/

11 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act -Section 3(c)(ii)," 2023.

12 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act -Section 2(z)," 2023.

13 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act -Section 10(2)(a)," 2023.

14 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act -Section 10(2)(c)(i)," 2023.

15 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act -Section 10(2)(b)," 2023.

16 Ministry of Electronics and Information Technology, " Indian Computer Emergency Response team (CERT-In)," https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

17 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act -Section 8(7)(a)," 2023.

18 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act -Section 6," 2023.

19 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act -Section 8(6)," 2023.

20 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act -Section 8," 2023.

[21] Ministry of Electronics and Information Technology, “Digital Personal Data Protection Act -Section 8(6),” 2023.

[22] Ministry of Electronics and Information Technology, “Digital Personal Data Protection Act -Section 6(3),” 2023.

[23] Ministry of Electronics and Information Technology, “Digital Personal Data Protection Act -Section 6,” 2023.

[24] Ministry of Electronics and Information Technology, “Digital Personal Data Protection Act -Section 11,12,” 2023.

[25] Ministry of Electronics and Information Technology, “Digital Personal Data Protection Act -Section 8(7),” 2023.

Key Takeaways

Vaishnavi Sharma

The DPDP Act 2023 has changed the regulatory landscape for data protection in India by providing for a comprehensive data governance structure, replacing sectoral and fragmented regulation of personal data. This legislation requires healthcare facilities to establish and maintain robust data protection mechanisms and security protocols, even if specific rules or regulations for managing health data remain absent. Healthcare entities should thereby invest in organisational and technological infrastructure to comply with these requirements.

While academia and industry widely agree that the DPDP Act implicitly includes individuals' health data under its definition of 'personal data,' a gap remains in its practical implementation in the healthcare sector due to the absence of sector-specific regulations. This regulatory ambiguity raises

concerns that data fiduciaries may either fail to establish adequate mechanisms for data usage and management or else create ineffective solutions.

At present, there is no clear governance framework for regulating health data use and management. The DPDP Act only addresses certain data-related mechanisms such as consent and notice frameworks, leaving broader governance issues unresolved.[a]

Challenges, Implementation, and Impact

Common challenges

One of the key challenges is the legislation's failure to explicitly recognise 'health' as a special category of data, which could result in oversight issues. The Act also does not clearly define 'harms', leaving no normative framework with which to categorise potential risks.

Start-ups and small- and medium-sized enterprises are also likely to face obstacles due to the operational complexity and compliance costs of the DPDP Act, particularly since many do not have established privacy mechanisms. The strict mandates, such as reporting data breaches to the Data Protection Board (DPB) and each affected data principal,[1] compound these challenges. Larger healthcare facilities, for their part, may be able to handle these demands more effectively by allocating additional resources.

Finally, India's health data governance policy ecosystem remains highly fragmented, comprising various guidelines, policies, and legislations, like the Health Data Management Policy and the Ayushman Bharat Digital Mission stack. It is crucial to delineate how these sector-specific initiatives will interact with the DPDP Act, especially given their collective focus on overseeing private-sector health service delivery. The absence of clear and specific guidelines adds to the uncertainty surrounding the law's practical implementation, potentially heightening challenges in achieving compliance and operational effectiveness.

It is still unclear whether primary oversight and governance responsibilities in the health sector will lie with the DPB, the Ministry of Health and Family Welfare, or authorities like the National Health Authority. This ambiguity could lead to inefficiency and confusion, as entities may have to seek multiple approvals or address queries from a number of regulatory bodies.

---

[a] It is imperative to note that for the healthcare sector specifically, the GDPR, for instance, is read along with other important rules and regulations, such as the eHealth Network initiative (voluntary), EU Directive on Security of Network and Information Systems, and the recently enacted EU AI Act. India, presently, does not have corresponding policies or rules to the DPDPA, making the regulatory landscape more uncertain.

Common Recommendations/Vision

First, as the two preceding chapters highlight, there is an urgent need to harmonise legal and policy frameworks across the healthcare sector, to offer clear and definitive guidance on key aspects of data protection. Specifically, this involves clearly establishing the regulatory structure for data governance amidst fragmented healthcare policies, and delineating the powers and scope of regulatory bodies to ensure consistent application and oversight across the sector.

Second, in the absence of specific health data-oriented regulations, healthcare facilities should identify and adopt best practices observed in other jurisdictions. These practices can serve as a benchmark for ensuring that data protection measures are robust and effective. This proactive approach is essential for maintaining compliance and avoiding potential penalties, thereby safeguarding the integrity of data protection efforts.

Addressing these areas will enable healthcare organisations to navigate the complexities of implementing the DPDP Act 2023 more effectively, ensuring they meet regulatory expectations and protect health data.

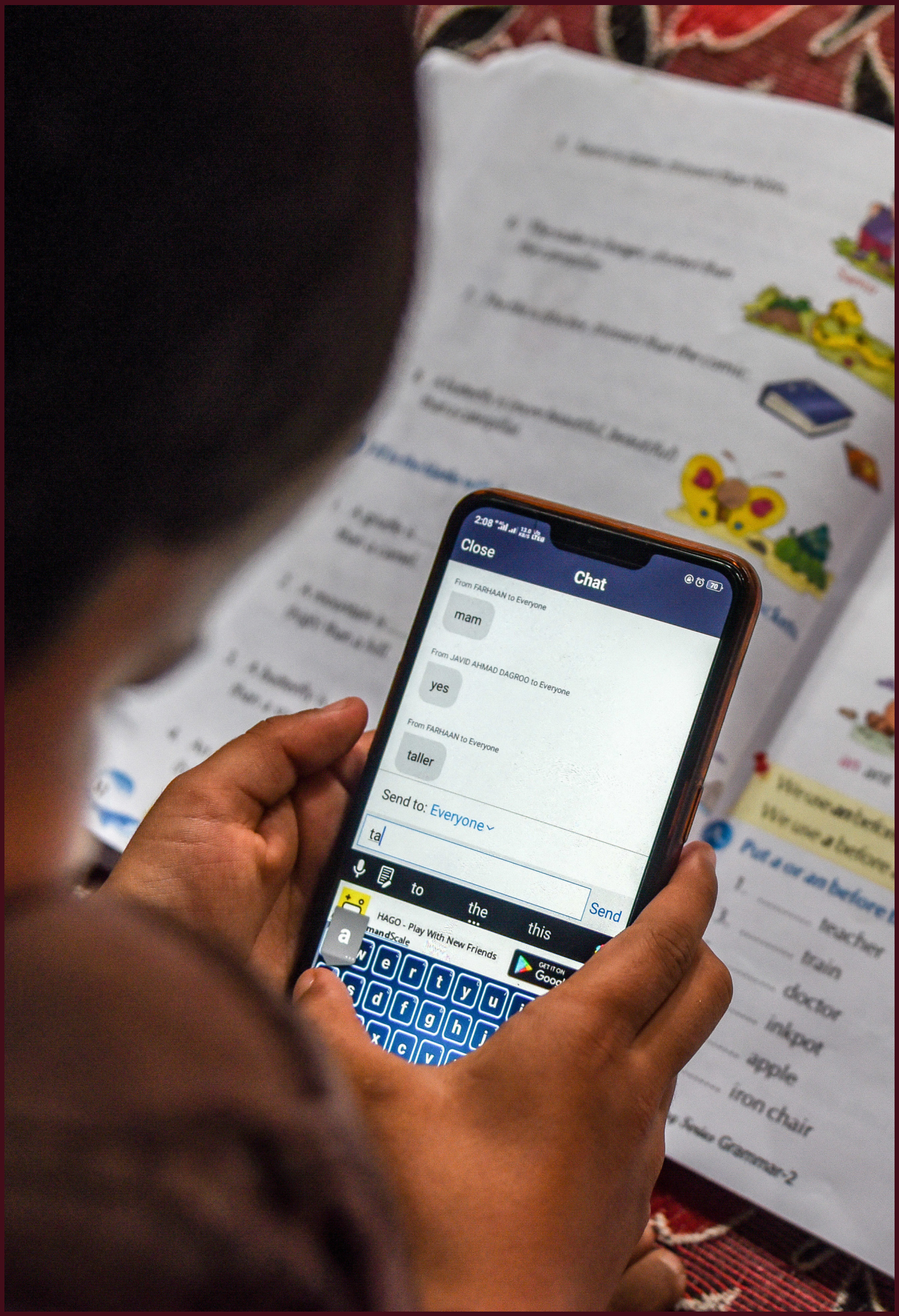
Conclusion

Given the current regulatory uncertainty surrounding the DPDP Act 2023 and the absence of detailed implementation guidelines, exploring collaboration between academia and industry becomes essential. Such collaboration is crucial for multiple reasons: (i) it provides a platform for diverse stakeholders to voice their concerns and exchange expertise on both the theoretical underpinnings of the Act and its practical applications; (ii) it establishes interim provisional guidelines on best practices for implementation, including technological standards that various healthcare players can adopt, based on their size and capacities; and (iii) it demonstrates a fundamental principle of the Act, which aims to recognise the diverse requirements and capabilities of stakeholders while mandating corresponding obligations.

Vaishnavi Sharma is Research Associate, The Dialogue.

Endnotes

1 Digital Personal Data Protection Act, 2023, Sec. 8(6).


Close
Chat
From FARHAAN to Everyone
mam
From JAVID AHMAD DAGROO to Everyone
yes
From FARHAAN to Everyone
taller
Send to: Everyone
ta
to
the
this
Send
HAGO - Play With New Friends
teacher
train
doctor
inkpot
apple
iron chair

04

EDUCATION AND CHILDREN'S DATA

Academic Perspective

Bilal Mohamed, Christina Michelakaki, and Dominic Paulger

An Application Perspective

Kathikeyan Balakumar, Kapish Saraf, Navneet Kishor Bharti, Sachit Dixit, and Savar Sharma

---

Key Takeaways

Prateek Tripathi

Academic Perspective

Bilal Mohamed, Christina Michelakaki, and Dominic Paulger

The Digital Personal Data Protection Act, enacted on 7 August 2023, comes at a critical juncture for India's growing education technology (edtech) services sector,[1] whose value is projected to reach US$10.5 billion by 2025.[2] This growth is driven by increased internet access, declining internet costs, and the shift to hybrid learning models following the COVID-19 pandemic.[3] As the sector evolves, it must reconcile its data-driven innovations with the privacy safeguards mandated by the new legislation.

A key challenge lies in the edtech industry's dependence on collecting, storing, and processing students' data. This chapter examines the DPDP Act's new provisions on children's personal data, particularly the requirement for parental consent, posing significant implications for how edtech companies operate and deliver services to young learners.

The Act's Framework for Regulating Children's Personal Data

Section 9 of the DPDP Act outlines three key obligations for data fiduciaries handling children's[a] personal data:[4]

- Data fiduciaries must obtain 'verifiable parental consent' (VPC) from a parent or lawful guardian before processing a child's personal data.
- The DPDP Act prohibits data fiduciaries from engaging in processing that is "likely to cause any detrimental effect on the well-being of a child."
- The DPDP Act mandates that data fiduciaries ensure that children's personal data is not used for "tracking," "behavioural monitoring," or "targeted advertising" directed at them.

These obligations apply to all entities processing digitised personal data within India, as well as to organisations outside of India that process personal data to offer goods or services to data principals in India.[5] Non-compliance may attract penalties of up to INR200 crore (approximately US$2.4 million).[6] Further details on compliance are anticipated in the forthcoming rules to be issued by the Central Government under Section 40 of the DPDP Act (DPDPA Rules).

Sections 9(4) and 9(5) of the DPDPA empower the Central Government to exempt certain data fiduciaries (potentially including edtech service providers) from the first and third obligations or to modify the age threshold for compliance. The upcoming DPDPA Rules are expected to clarify key terms and establish criteria for determining when processing is considered "verifiably safe."[7] However, without these rules, the scope of these requirements remains unclear, posing compliance challenges for data fiduciaries.

Challenges in Operationalising the Act's Provisions

a. **Lack of clarity in complying with the DPDP Act's VPC requirement may lead to over- or undercompliance.**
   The lack of clear guidance on the DPDP Act's verifiable parental consent (VPC) requirement poses challenges for India's edtech sector, especially for startups. This uncertainty may result in two possible outcomes:

   - **Overcompliance:** Some edtech companies, out of caution, may implement stricter compliance measures than required by the DPDP Act. While this approach reduces legal risks, it could increase operational costs, limiting resources for innovation and potentially stifling growth.

[a] Defined as individuals under 18 years old.

- **Undercompliance:** Conversely, some organisations may adopt a more relaxed approach due to the lack of clarity, resulting in inadequate verification processes. This undermines the DPDP Act's primary goal of protecting personal data.

In both scenarios, the lack of legal certainty risks hindering the development of educational technologies that could benefit India's youth. It also risks creating an uneven playing field for organisations within the edtech space.

b. Practical challenges in implementing age assurance and consent verification measures in India's unique socio-technological context.

Global edtech companies may already have systems in place to verify user ages and obtain VPC to comply with data protection laws and regulations.[8] However, adapting these measures for India presents significant challenges due to the country's distinct socio-technological landscape.

- **Digital Divide:** India faces a significant digital divide, characterised by low digital literacy rates and disparities in internet access between rural and urban areas. For instance:A 2023 survey by the National Sample Survey Office found that only 27.5 percent of individuals aged 15-29 were classified as "digitally skilled".[9]
- **Device Sharing:** Many Indian households have several family members sharing a single device,[10] complicating the implementation of traditional parental consent mechanisms.
- **Linguistic Diversity:** Given the complexity of age verification and parental consent processes, user interfaces must be sensitive to linguistic diversity and regional nuances, providing clear and easily understandable information. Section 5(3) of the DPDP Act acknowledges this challenge, requiring data fiduciaries to provide notices in English or any of the 22 languages specified in the Eighth Schedule of the Constitution.

These factors may increase the likelihood that VPC measures may be circumvented or that VPC will not be obtained effectively within the Indian context. Therefore, both regulators and edtech companies must explore innovative approaches to implementing the VPC requirement. These approaches should address India's unique challenges while meeting the data protection objectives outlined by the DPDP Act.

c. Age assurance and consent verification measures currently under consideration by the Indian Government may increase costs for edtech companies.

In implementing the DPDP Act's VPC requirement, the Central Government

must foster an environment that supports innovation in the edtech sector by ensuring that the proposed solutions are accessible and feasible for edtech providers of all sizes.

Certain VPC mechanisms currently under consideration by the Government could inadvertently create new challenges for India's edtech sector. Implementing third-party verification measures could raise operational costs for edtech providers, particularly impacting startups and smaller companies.[11] Integrating third-party technology could take several weeks and increase unit costs or annual expenditures, depending on the billing model.

In the United States (US), startups have incurred costs of up to US$10,000 to integrate such technology. Since parental consent through DigiLocker has yet to be operationalised, the associated costs remain unclear. However, it is crucial to note that DigiLocker is a voluntary service, and mandating its use for parental consent may not meet the proportionality test in *Justice K.S. Puttaswamy vs. Union of India.*

d. Prohibition on tracking, behavioural monitoring, and targeted advertising could impact edtech providers' ability to collect children's data for beneficial purposes.

While the DPDP Act's prohibition on tracking, behavioural monitoring, and targeted advertising aimed at children seeks to protect their privacy, a blanket ban may overlook the benefits of responsible user profiling in educational contexts. Without specific carve-outs for educational purposes, this prohibition could hinder edtech providers' ability to collect children's data for creating personalised learning experiences—such as identifying individual strengths and weaknesses or curating age-appropriate content. This limitation may restrict edtech service providers from delivering more targeted and effective educational services.[12]

International Landscape

The implementation of the DPDP Act is at a critical juncture. With the DPDPA Rules yet to be notified, the Ministry of Electronics and Information Technology (MeitY) has a significant opportunity to clarify the operationalisation of the Act's provisions, particularly concerning children's data protection in the edtech sector. Below is a comprehensive examination of children's data protection laws across several key jurisdictions. This analysis examines how these jurisdictions implement parental consent requirements, aiming to identify best practices that can help ensure India's data protection framework effectively protects children's data while fostering innovation in the edtech sector.

European Union (EU) and the United Kingdom (UK)

Effective from May 2018, the General Data Protection Regulation (GDPR) governs the

processing of personal data in the EU.[b] Following Brexit, the UK implemented its version of the GDPR, which largely mirrors the EU GDPR but operates independently of EU law and may diverge from it in the future. Furthermore, the "Brussels effect"[13] means that the GDPR, along with its predecessor, Directive 95/46/EC, have influenced the development of various emerging data protection laws globally.

The GDPR establishes a unified set of data protection rules for all EU Member States while allowing limited flexibility for individual countries to adapt certain rules to their national contexts. These rules encompass general rights and obligations regarding personal data processing, as well as specific provisions governing the processing of children's personal data.

Article 8 of the GDPR states that when a provider of an "information society service" (ISS)[c] offered directly to children relies on consent as the lawful basis for processing a child's personal data, the child can only lawfully provide consent if they are 16 years or older.[14] However, EU Member States have the option to lower this age to 13.[d]

Importantly, Article 8 specifies that ISS providers must seek parental consent only if: (1) they intend to rely on consent to process the child's personal data, rather than another lawful basis under Article 6 of the GDPR (such as "legitimate interests"); and (2) the child is below the age established by the relevant EU Member State (which can be as young as 13 years old). When relying on parental consent, controllers must "make reasonable efforts to verify that the consent is given or authorised by the holder of parental responsibility over the child," considering available technology.[15]

National data protection authorities (DPAs) in Europe are focusing on protecting student data privacy.[16] Some DPAs have issued guidance on EdTech under the GDPR. A notable example is the set of guidelines issued by the UK's Information Commissioner's Office (ICO).[17] These guidelines confirm that under the UK GDPR, edtech providers may process children's personal data without seeking parental consent if the organisation can demonstrate that an alternative lawful basis to consent, such as legitimate interests, is applicable.[18]

---

[b] In parallel with the GDPR, Member States may have sectoral legislation concerning education.

[c] Defined as a service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services (GDPR, Article 4(25); Directive (EU) 2015/1535, Article 1(1)(b)).

[d] For a list of countries that have lowered the age for children's consent, see https://www.skillcast.com/blog/gdpr-age-consent-not-childs-play

The United States (US)

In the US, the Children's Online Privacy Protection Act (COPPA)[19] governs how commercial operators collect and use personal information from children under 13.

On "child-directed" sites, operators who have actual knowledge that a user is under 13 must obtain verifiable parental consent before collecting or using children's information.[20] Under guidance from the Federal Trade Commission, schools may consent on behalf of parents to allow third parties to collect student personal information solely for school purposes, not for commercial purposes.[21] In this situation, the third party must still provide the school with required notices, descriptions of the types of personal information collected, an opportunity to review or delete the collected information, and a chance to stop the collection of the child's personal data.[22]

Several US states have enacted student privacy laws,[23] with California's Student Online Personal Information Protection Act (SOPIPA) (2014),[24] among the most notable. Many other states have modeled their privacy laws after SOPIPA. Under SOPIPA, and similar laws, education technology vendors cannot request parental consent for using student data for prohibited purposes, such as commercial purposes.[25] Additionally, state laws often mandate employee training on data security and privacy policies related to student data.[26] They may also impose stringent requirements for contractual clauses concerning student data privacy in agreements between schools and edtech vendors, thereby enhancing protections.[27]

Singapore

Singapore governs its data protection framework through the Personal Data Protection Act (PDPA), enacted in 2012 and amended in 2020. While the PDPA does not impose specific obligations for processing children's personal data, Singapore's data protection authority, the Personal Data Protection Commission (PDPC), has issued two sets of guidelines regarding the application of the PDPA to children's data processing in both the edtech sector and other contexts: (1) the Advisory Guidelines on the PDPA for Selected Topics[28] and (2) the Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment, which specifically target organisations whose online products or services are likely to be accessed by children.[29]

These guidelines clarify that, although the age of majority under Singapore's common law is 21 years old, the PDPC generally recognises individuals aged 13 and above as capable of providing consent for the processing of their personal data. The guidelines urge organisations to ensure that minors understand the nature and consequences of sharing their personal data, encouraging the use of easily understandable language. If an organisation believes that a minor lacks sufficient understanding or is below 13 years of age, it must seek consent from the minor's parents or legal guardians.

These guidelines also grant organisations flexibility in selecting suitable age assurance methods. While the PDPC encourages organisations to use such methods to implement safeguards for child users, it does not mandate the adoption of any specific methods.

Brazil

Brazil's primary data protection law, the Lei Geral de Proteção de Dados (LGPD), enacted in 2018 and effective from 2020, establishes rights and obligations concerning the processing of personal data, specifically protecting the personal data of children and adolescents. Article 14 of the LGPD mandates that controllers obtain the consent of a child's parent or legal guardian before processing the child's personal data. Notably, the LGPD itself does not define children or adolescents.

On 24 May 2023, Brazil's data protection authority, the Autoridade Nacional de Proteção de Dados (ANPD), issued a statement to clarify the legal bases available for processing children's and adolescents' personal data. According to CD/ANPD Statement No. 01/2023, personal data of children and adolescents may be processed under the legal bases outlined in Articles 7 and 11 of the LGPD, including legitimate interests, legal obligations, and research.[30] On 2 February 2024, the ANPD published a guide on the practical application of legitimate interests as a ground for processing non-sensitive personal data.[31] This guide recognises legitimate interests as a legal basis for processing children's and adolescents' data, provided that the entity processing the data ensures their best interests. To this end, the data controller (data fiduciary) must document how they consider the child's best interest, the criteria used and ensure that no excessive risks or impacts arise.

South Africa

The Protection of Personal Information Act (POPIA)[32] is South Africa's data protection law, enacted in 2013, with most provisions effective from July 2020, followed by one-year grace period for compliance. Like other data protection laws, it establishes general rights and obligations for processing personal data, with specific provisions for children's personal data.[e]

The POPIA prohibits processing of children's personal data,[33] with exceptions, such as when a "competent person" (usually a parent or legal guardian) consents to the processing.[34]

[e] POPIA defines a "child" as a person under the age of 18 who lacks the legal competence, without the assistance of a competent person, to make any decisions regarding any matter concerning themselves. This definition considers not only an individual's age but also their capacity to make independent decisions about how their personal information is processed.

Comparison

The regulation of children's data protection varies across jurisdictions, particularly regarding age thresholds and the necessity of parental consent. Across the jurisdictions presented above, the requirement for parental consent is nearly universal. However, many jurisdictions—including the EU, UK, Brazil, and Singapore—recognise alternative legal bases for processing children's data, especially in educational contexts.

The age threshold for requiring parental consent varies across jurisdictions, ranging from 13 to 18, with some offering more flexibility than others. This evolving landscape reflects a growing awareness of the need to balance data protection with the benefits of digital services for children, particularly in education.

Recommendations

India's National Education Policy identifies "extensive use of technology in teaching and learning" as a key priority. When developing rules to implement Section 9 of the DPDPA, the government must balance protecting children's personal data with fostering growth and innovation in the edtech sector. Restrictive measures could deprive young people of the substantial educational benefits that innovative edtech solutions offer. Below are the recommendations for implementing the law.

- **Include edtech services within classes of data fiduciaries that must be exempt from Section 9(1) and 9(3) in providing educational services.**

To ensure a proportionate, risk-based approach, the Central Government should consider exempting edtech providers from obtaining VPC and allow exceptions for behavioural tracking and monitoring when the processing is solely for delivering educational services, provided they meet standards and criteria to ensure protections. Under Section 9(4), the Central Government can impose certain conditions on specific data fiduciaries. This could involve prescribing higher standards, including data minimisation obligations, transparency requirements, individual rights such as access, correction, and erasure. Further accountability measures could include appointing a data protection officer and designing age-appropriate platforms.[35]

- **Lower the age of consent for data fiduciaries that design children-friendly gateways for education.**

While recommending the inclusion of edtech providers within the class of data fiduciaries exempt from obligations under Section 9(1) and (3) of the DPDP Act, the Central Government should consider lowering the age for obtaining parental consent for platforms that host children-friendly gateways for educational content in a "verifiably safe" manner. By ensuring enhanced transparency and digital literacy

for parents and children, implementing privacy-friendly default systems, and enforcing strict data-sharing practices, the Government can safeguard the best interests of the child.[36]

- **Consider providing edtech companies with targeted exemptions from the prohibition on tracking and behavioural monitoring of children in Section 9(3) of the DPDP Act.**

While the intent behind Section 9(3) of the DPDP Act is commendable, this provision may hinder the effectiveness of edtech services. A more nuanced approach could allow tracking and behavioral monitoring of children for educational purposes, while safeguards addressed through existing DPDP Act provisions. For instance, the prohibition on processing children's data in ways that harm their well-being already establishes a baseline level of protection. Additionally, concerns about the commercialisation of children's data could be mitigated by imposing restrictions on targeted advertising aimed at children.

- **Provide flexibility in age assurance and VPC methods that can demonstrate compliance with Section 9(1) of the DPDP Act.**

Flexibility is essential, given India's unique socio-technological context, which differs from that of other jurisdictions, like the US, where mechanisms for age assurance and VPC are more established among edtech providers. In low-risk scenarios, alternatives to parental consent that are proportionate to the use case may be beneficial. For example, in low-risk cases, age-gating or self-declaration may be appropriate, while in higher-risk scenarios, facial recognition or capacity testing might be more suitable.[37]

Conclusion

The enactment of the DPDP Act is a key milestone in India's data protection journey, signalling a transformative period for all stakeholders. The gap between the law's enactment and the notification of subordinate legislation presents a valuable opportunity for regulators to implement the law smoothly, promoting the protection of individuals' privacy while supporting the growth of various sectors.

Bilal Mohamed is Policy Analyst for Global Privacy, Future of Privacy Forum.

Christina Michelakaki is Policy Counsel for Global Privacy, Future of Privacy Forum.

Dominic Paulger is Deputy Director for Asia-Pacific, Future of Privacy Forum.

The authors thank Alexa Mooney, David Sallay, Gabriela Zanfir-Fortuna, Jim Siegl, Josh Lee Kok Thong, Lee Matheson, Mercy King'ori, and Rob Van Eijk for their contributions to this chapter.

Endnotes

1 Digital Personal Data Protection Act, 2023, Section 2(i)

2 Aishwarya Anand, "India's Edtech Market Expected to Grow to $10 Billion by 2025," CNBC TV 18, April 12, 2023, https://www.cnbctv18.com/education/india-edtech-market-expected-to-grow-to-10-billion-by-2025-startupsunicorns-16391151.htm

3 Annapurna Roy, "How India is Using the Internet," *The Economic Times,* March 10, 2024, https://economictimes.indiatimes.com/tech/technology/how-india-is-using-theinternet/articleshow/108354854.cms?from=mdr

4 Digital Personal Data Protection Act, 2023, Section 2(f)

5 Raktima Roy and Gabriela Zanfir-Fortuna, "The Digital Personal Data Protection Act of India, Explained," FPF Blog, August 15, 2023, https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/

6 Digital Personal Data Protection Act, 2023, Schedule under Section 33(1)

7 Bailey Sanchez et al., "Verifiably Safe" Processing of Children's Personal Data Under the DPDPA 2023: A Catalogue of Measures," Future of Privacy Forum And the Dialogue, 2023, https://fpf.org/wp-content/uploads/2023/11/Verifiably-safe-processing-of-childrens-personal-data-under-the-DPDPA-2023-A-Catalogue-of-Measures2.pdf

8 Future of Privacy Forum, "Verifiable Parental Consent Report & Infographic," FPF Blog, June 22, 2023, https://fpf.org/resource/fpf-releases-report-on-verifiable-parental-consent/

9 Nishtha Pandey, "NSSO survey | Only 31% Young Men in India can Send Emails with Attachments," CNBC TV 18, March 27, 2023, https://www.cnbctv18.com/education/nsso-survey--only-31-young-men-in-india-can-send-emails-with-attachments-16275661.htm

10 Rajesh Tandon, "One Device Households," The Times of India, July 17, 2020, https://timesofindia.indiatimes.com/blogs/voices/one-device-households/

11 Future Of Privacy Forum, Verifiable Parental Consent: The State of Play, 2023, https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf

12 Infosys BPM, "How Data Analytics Is Powering the EdTech Industry," https://www.infosysbpm.com/blogs/education-technology-services/how-data-analytics-is-powering-the-edutech-industry.html

13 Anu Bradford, The Brussels Effect, 107 Nw. U. L. Rev. 1 (2012), https://scholarship.law.columbia.edu/faculty_scholarship/271/

14 EU Regulation 2016/679 (General Data Protection Regulation), Article 8.

15 EU Regulation 2016/679 (General Data Protection Regulation), Article 8(2)

16 Molly Killeen, "Privacy Concerns Set to Grow With the Digitalisation of Education," Euractiv, July 30, 2021, https://www.euractiv.com/section/digital/news/privacy-concerns-set-to-grow-with-the-digitalisation-of-education/; Ayça Atabey and Louise Hooper, International Regulatory Decisions Concerning EdTech Companies' Data Practices, The Digital Futures for Children Centre, LSE and 5Rights Foundation, 2024, https://eprints.lse.ac.uk/123805/1/DFC_Brief_International_regulatory_decisions_final.pdf

17 Information Commissioner's Office, "The Children's Code and Education Technologies (edtech)," https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/the-children-s-code-and-education-technologies-edtech/

18 Information Commissioner's Office, "What Do We Need to Consider When Choosing a Basis for Processing Children's Personal Data?," https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-do-we-need-to-consider-when-choosing-a-basis-for-processing-children-s-personal-data/

19 Title 16, Code of Federal Regulations, Part 312, https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

20 Title 16, Code of Federal Regulations, 312.5(a)(1), https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312/section-312.5

21 "Complying with COPPA: Frequently Asked Questions," Federal Trade Commission Business Guidance Resources, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions

22 "Complying with COPPA: Frequently Asked Questions"

23 Student Privacy Compass, State Student Privacy Laws, https://studentprivacycompass.org/state-laws/

24 Student Online Personal Information Protection Act, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177

25 Brenda Leong et al., FPF Guide to Protecting Student Data Under SOPIPA, Future of Privacy Forum, 2016, https://fpf.org/wp-content/uploads/2016/11/SOPIPA-Guide_Nov-4-2016.pdf

26 See, for example, West Virginia Code Chapter 18. Education § 18-2-5h. Student Data Accessibility, Transparency and Accountability Act, https://codes.findlaw.com/wv/chapter-18-education/wv-code-sect-18-2-5h/

27 See, for example, New York Consolidated Laws, Education Law - EDN § 2-d. Unauthorized release of personally identifiable information, https://codes.findlaw.com/ny/education-law/edn-sect-2-d.html

28 Personal Data Protection Commission Singapore, "Advisory Guidelines on the Personal Data Protection Act for Selected Topics," 2024, https://www.pdpc.gov.sg/guidelines-and-consultation/2020/02/advisory-guidelines-on-the-personal-data-protection-act-for-selected-topics

29 "Advisory Guidelines on the Personal Data Protection Act for Selected Topics," 2024.

30 Diário Oficial Da União, Ministério da Justiça e Segurança Pública/Autoridade Nacional de Proteção de Dados/Conselho Diretor, Enunciado Cd/Anpd Nº 1, De 22 De Maio De 2023, https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf

31 Autoridade Nacional de Proteção de Dados, "Hipóteses legais de tratamento de dados pessoais legítimo interesse," Autoridade Nacional de Proteção de Dados, 2024, https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf

32 Protection of Personal Information Act, 2013 https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

[33] Protection of Personal Information Act, 2013, Section 34.

[34] Protection of Personal Information Act, 2013, Section 35(1)(a).

[35] "Verifiably safe," processing of children's personal data under the DPDPA 2023: A Catalogue of Measures

[36] "Verifiably safe," processing of children's personal data under the DPDPA 2023: A Catalogue of Measures

[37] Bailey Sanchez and Jim Siegl, "New FPF Infographic Analyzes Age Assurance Technology & Privacy Tradeoffs," FPF Blog, June 26, 2023, https://fpf.org/blog/new-fpf-infographic-analyzes-age-assurance-technology-privacy-tradeoffs/; Aparajita Bharti et al., "Navigating Children's Privacy and Parental Consent Under the DPDP Act 2023," The Quantum Hub, 2023, https://thequantumhub.com/wp-content/uploads/2023/11/TQH-YLAC-Childrens-Privacy-under-DPDP-Act-2023.pdf

An Application Perspective

Kathikeyan Balakumar, Kapish Saraf, Navneet Kishor Bharti, Sachit Dixit, and Savar Sharma

Countries and organisations have long relied on data for resource allocation and strategic planning. However, the success of these efforts depends on the availability of high-quality, actionable data for policymakers and on-the-ground personnel. When data is in silos across departments, the ability to drive meaningful change diminishes.[1] In recent decades, computers and the internet have transformed data management, enabling information centralisation and unlocking vast economic, political, and social potential.[2] Yet, this centralisation of data has also introduced risks, with data breaches becoming increasingly common, threatening the security and privacy of sensitive information.[3]

Reports[4] indicate that the education sector was "by far the largest impacted" by data breaches, accounting for over 50 percent of all incidents. Measures such

as data minimisation, prompt breach notifications, and implementing robust security measures, as outlined in the Digital Personal Data Protection Act, 2023,[a] could help reduce these risks. As the value of data continues to rise, the frequency and severity of such incidents are only expected to grow, making digital data protection legislation essential.

It is crucial to recognise that many benefits within educational institutions arise from the availability of data for peer review,[b] critique, debate, sharing, and intellectual growth. Overly stringent privacy regulations could obstruct data, potentially prevent the programme's implementation, and limit the sharing of best practices among principals and other stakeholders. While the DPDP Act aims to reduce the risks from data breaches and unauthorised access, enhancing trust in digital systems, it is equally important to ensure that its implementation does not inadvertently hinder the innovation and collaboration necessary for advancing educational and social initiatives.

Industry Standards and Expectations

India's education industry is diverse,[c] covering well-funded urban universities and small schools in rural districts with limited infrastructure. This diversity makes it challenging to develop industry standards that are both comprehensive and adaptable to these differing needs. Despite significant investments, the focus often remains on meeting basic requirements rather than striving for excellence, with many primary schools still struggling with access and basic literacy, leaving little room for data-driven innovation. Implementing the DPDP Act must consider these disparities to avoid exacerbating existing inequalities. If implemented hastily, regulations may allow wealthier institutions to comply and enhance data capabilities, while rural institutions would struggle to meet compliance requirements, widening the gap. To avoid such outcomes, the DPDP Act must adopt a balanced approach that considers the unique challenges faced by different types of educational institutions.

---

a Legislations like the DPDP Act aim to establish a comprehensive framework for the secure collection, processing, and storage of personal data, providing clear guidelines and enforcing stringent measures to reduce the risks of breaches and unauthorised access.

b For instance, the Mid-Day Meals scheme, which aims to enhance nutrition and educational outcomes for children in India, depended heavily on analysing data related to student attendance, social backgrounds, educational status, nutritional status, and academic performance (Chen, 2024).

c Varying in size, specialisations, and available resources.

The rules and standards suitable for one type of educational institution may not work for another. For instance, technical education relies on detailed student performance data to tailor training programmes and ensure practical competency, often requiring tracking of progress in lab assignments and technical projects. This necessitates strict security measures to safeguard both intellectual property and personal information. In contrast, management education prioritises behavioural data, focusing on leadership potential, teamwork, and decision-making skills.

Educational institutions prioritise individual development over profit. To educate effectively, teachers need insight into their students' academic performance, learning styles, and personal challenges, which rely on access to detailed data. Embracing data-driven insights requires educators to move beyond traditional insecurities about data sharing and adopt an open, forward-thinking mindset. This shift fosters an environment where both teachers and students thrive. In this setting, data supports personalised education, enabling tailored learning experiences that address individual needs and enhance overall progress.

Therefore, as the DPDP Act is implemented, it must account for the education sector's unique needs, supporting the overarching goal of improving educational outcomes nationwide. This will require a balanced approach that safeguards data while ensuring accessibility and innovation in education.

Given the education sector's unique landscape, there are several key expectations the industry holds for a legislation like the DPDP Act:

1. **Flexibility in application:** The DPDP Act should be adaptable to the diverse needs of various educational institutions. Whether a large university or a small school in a rural region, the law should allow for tailored implementation that addresses each institution's unique context and challenges.

2. **Support for data-driven education:** The Act should not only protect data but also enable its use to enhance educational outcomes. This includes facilitating personalised education, early intervention for at-risk students, and the development of innovative educational programs.

3. **Balance between security and accessibility:** While personal data protection is crucial, the DPDP Act should ensure that data remains accessible to educators and researchers. Clear guidelines must be set for sharing data responsibly within the academic community without compromising privacy.

4. **Clear guidelines for different educational sectors:** The Act should acknowledge the distinct needs of various educational sectors. For example, technical education may require stringent protection for intellectual property, while

management education may focus on behavioural data. The DPDP Act should provide sector-specific guidelines to address these differences.

5. **Encouragement of collaboration and innovation:** The DPDP Act should encourage collaboration between institutions, researchers, and policymakers by establishing secure, privacy-compliant data-sharing frameworks. This collaboration is essential for scaling successful educational programmes and adapting them to different contexts.

6. **Support for institutional growth and development:** The DPDP Act should serve not only as a regulatory tool but also as a framework that supports the growth and development of educational institutions. By enabling secure yet flexible data management, the Act can help institutions innovate, improve their offerings, and better serve their students.

By meeting these expectations, the DPDP Act can play a pivotal role in protecting personal data while fostering an educational environment that promotes security, growth, collaboration, and innovation.

Challenges, Implementation, and Impact

Before the DPDP Act, data management in the education sector was often fragmented, hindering both data privacy and opportunities for growth through data-driven decision-making. The DPDP Act is now compelling institutions to adopt standardised data management practices, essential for enhancing stakeholder trust, encouraging digital learning, and enabling informed decision-making with accurate, securely managed data. However, achieving full compliance with the legislation remains a significant challenge.

This section highlights the critical challenges educational institutions may face in implementing the DPDP Act. These include difficulties in obtaining explicit consent, inadequate IT infrastructure, and balancing data minimisation with analytical requirements. Restrictions on data use could hinder research and innovation, while ensuring third-party compliance adds complexity. Additional challenges stem from the sector's diversity, the need to balance data protection with educational flexibility, technological and financial constraints, risks of data breaches, and cultural resistance to change. Addressing these issues is essential for educational organisations to implement the DPDP Act effectively and maximise its benefits.

Table 1 outlines innovative solutions to challenges and explores how effective implementation of the DPDP Act could help mitigate their impact.

Table 1: Challenges and Proposed Solutions

Challenge	Description	Proposed Solutions	Potential Impact
Cost Implications	Upgrading IT infrastructure and implementing DPDPA-	• **Cost-Sharing Models:** Promote collaboration among institutions to share IT resources. • **Government Subsidies:** Seek government grants to alleviate financial strain.	**Moderate Impact:** Cost-sharing and government support can alleviate the financial burden, enabling wider compliance. However, disparities between well-funded and under-resourced institutions may remain.
Managing Non-Educational Tasks	Tasks like placements, scholarships, and workshops involve data sharing with external parties, posing challenges for DPDPA compliance.	• **Clear Data Sharing Agreements:** Establish comprehensive data-sharing protocols with third parties, ensuring compliance with DPDPA. • **Role-based Access Controls:** Limit data access based on roles and necessity.	**Moderate Impact:** Well-defined agreements and access controls can mitigate risks, but ensuring third-party compliance remains challenging, particularly when dealing with multiple vendors and stakeholders.
Overburdening Educators	The act could concentrate data management responsibilities on a small group of educators, potentially overburdening them.	• **Data Management Teams:** Form dedicated teams for data management to distribute responsibilities. • **Training and Support:** Provide continuous training and resources to educators on data management best practices and DPDPA compliance.	**Moderate Impact:** Forming specialised teams can distribute the workload, but smaller institutions with limited staff may still face challenges. Ongoing support and training are crucial for sustaining this approach.

Cultural Resistance to Change	There may be resistance from staff and students who are accustomed to traditional data management practices.	• **Change Management Programs:** Implement structured programs to guide staff and students through the transition. • **Leadership Engagement:** Involve institutional leaders in promoting the importance of the DPDPA.	**Moderate Impact:** Effective change management can reduce resistance, but its success depends on the active engagement and commitment of both leadership and the broader educational community to adopt new practices.
Data Sharing and Collaboration Restrictions	The DPDPA could restrict data sharing, potentially hindering academic collaboration and research.	• **Anonymisation Techniques:** Use data anonymisation to allow safe sharing of information. • **Controlled Data Access:** Implement time-limited and purpose-specific data access protocols to facilitate collaboration.	**Moderate Impact:** Anonymisation and controlled access can maintain collaboration while protecting data. However, balancing data utility with protection needs careful management to ensure academic and research objectives.
Balancing Data Protection with Educational Flexibility	The need to protect data might conflict with the flexibility required for educational activities, such as personalised learning.	• **Flexible Compliance Frameworks:** Develop frameworks that enable flexible data use while maintaining strict protection protocols. • **Pilot Programs:** Implement pilot programs to test and refine flexible data use policies.	**Moderate Impact:** Flexible compliance frameworks can support educational activities, but continuous monitoring is required to prevent potential breaches. Pilot programs can help identify best practices before broader implementation.

Data Management for Minors	Educating minors raises concerns about their level of consent and exercise agency in data sharing and management.	• **Parental Consent Protocols:** Implement robust parental consent processes. • **Age-Appropriate Data Handling:** Develop guidelines for handling data specifically for minors, considering their limited agency.	**Significant Impact:** Clear protocols for parental consent and handling minor-specific data can ensure compliance and protect vulnerable populations. However, this may require additional resources and administrative efforts to manage effectively.
Ensuring Vendor Compliance	Reliance on third-party vendors for services such as Learning Management Systems and cloud storage adds complexity in ensuring DPDPA compliance.	• **Vendor Audits:** Regular audits of vendors to ensure DPDPA compliance. • **Contractual Obligations:** Include strict data protection clauses in contracts with vendors.	**Significant Impact:** Vendor compliance is critical for data security. While rigorous audits and contracts can help, maintaining consistent compliance across all vendors may prove challenging, especially for institutions with limited oversight capacity.

Technological and Infrastructural Constraints	Some institutions may lack the necessary technology or infrastructure to comply with the DPDPA.	• **Infrastructure Grants:** Advocate for government and private sector grants to upgrade IT infrastructure. • **Cloud Solutions:** Leverage secure cloud services to reduce the need for extensive on-premises infrastructure.	**Significant Impact:** Grants and cloud solutions can alleviate technological constraints, but reliance on external funding and services may introduce risks, such as dependency on specific vendors or technology platforms.
Difficulty in Obtaining Explicit Consent	Obtaining and managing explicit consent for data use, especially from diverse student populations, can be complex.	• **Digital Consent Platforms:** Utilise digital platforms to streamline the process of obtaining, managing, and tracking consent efficiently. • **Consent Education Campaigns:** Educate students and parents on the importance of data consent.	**Significant Impact:** Streamlined digital consent processes can enhance compliance, but ensuring full understanding and engagement from all stakeholders, particularly in large and diverse institutions, remains a challenge.

Source: Authors' own

Recommendations

To ensure successful DPDP Act implementation within the education sector, stakeholders must adopt a structured approach that fosters both inter-and intra-industry collaboration. Such collaborations have been key to successful data regulations, such as the General Data Protection Regulation in the European Union (EU) and Singapore's financial sector regulations. Institutions should start with a comprehensive data audit to identify compliance gaps, followed by the establishment of clear data governance policies aligned with the DPDP Act. Upgrading IT infrastructure with security measures like encryption and secure cloud storage is vital to protect sensitive data and build stakeholder

trust.[5] Regular training for staff on data minimisation, consent management, and secure data handling will enhance compliance.[6] Moreover, creating platforms or committees for collaboration between educational institutions, technology providers, and regulatory bodies can drive innovative solutions and address common challenges.[7] Continuous monitoring and regular reviews of data management practices are essential to ensure ongoing compliance with the law.

Policymakers can further enhance industry support for DPDP Act implementation in the education sector through targeted policy directions. Collaborative innovation policies can promote industry-university partnerships to drive technological advancements.[8] Industry engagement regulations should ensure regulatory integrity and accountability. Technology adoption incentives, such as tax incentives, can accelerate the integration of secure data management systems. Capacity-building initiatives, including staff training programmes, are essential for promoting secure data management. Sector-specific support programmes tailored to address unique educational challenges can provide the necessary resources and guidance to bolster DPDP Act implementation.

By implementing these practices and policy directions, educational institutions can effectively navigate the challenges posed by the DPDP Act while strengthening data security and promoting effective data management. This comprehensive approach will ensure regulatory compliance while fostering a culture of accountability, transparency, and continuous improvement. It will help create a safe and supportive learning environment for students to thrive academically and personally in the digital age.

Conclusion

The DPDP Act's introduction is momentous for India's education sector, compelling institutions to adopt stricter and standardised data management practices. While crucial for protecting student data, enhancing stakeholder trust, and enabling data-driven decisions, achieving full compliance presents challenges. These include the financial burden of IT upgrades, complexities in obtaining and managing consent, and ensuring third-party compliance, all of which demand careful and strategic navigation.

These challenges, however, are not insurmountable. Institutions can adopt innovative solutions—such as cost-sharing models, digital consent platforms, and flexible compliance frameworks to implement the DPDP Act effectively while preserving the flexibility essential for educational innovation. Collaboration among educators, policymakers, and technology providers will be crucial to address these challenges and ensure that the benefits of the DPDP Act are fully realised.

The successful implementation of the DPDP Act will protect the privacy and security of personal data while reshaping the education sector. It will foster a culture of accountability, transparency, and continuous improvement. By adapting to this new regulatory landscape, institutions can create safer, more supportive learning environments, empowering students to thrive academically and personally in an increasingly digital world.

Karthikeyan Balakumar is Assistant Professor of Marketing and Chairperson of Placements and Career Development, IIM Sirmaur.

Kapish Saraf is the Founder and CEO of KidEx, an experiential learning edtech platform for schools and colleges.

Navneet Kishor Bharti is a final-year MBA student (2023-2025 batch), IIM Sirmaur.

Sachit Dixit is a final-year MBA student (2023-2025 batch), IIM Sirmaur.

Savar Sharma is a final-year MBA student (2023-2025 batch), IIM Sirmaur.

Endnotes

1 Keren Naa Abeka Arthur and Richard Owen, "A Micro-Ethnographic Study of Big Data-Based Innovation in the Financial Services Sector: Governance, Ethics and Organisational Practices," in *Business and the Ethical Implications of Technology* (Springer, 2022), 57–69.

2 Al Sentot Sudarwanto and Dona Budi Kharisma, "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia," *Journal of Financial Crime* 29, no. 4 (2022): 1443–57.

3 Jozef Andraško et al., "The Regulatory Intersections Between Artificial Intelligence, Data Protection and Cyber Security: Challenges and Opportunities for the EU Legal Framework," *AI and Society* 36, January 2, 2021.

4 Verizon, "Verizon 2024 Data Breach Investigations Report," 2024, https://verizon.com/dbir.

5 Bing Chen and Yongji Liu, "Promotion and Advancement of Data Security Governance in China," *Electronics* 13, no. 10 (2024): 1905.

6 Sudarwanto and Kharisma, "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia."

7 Yi-Shan Tsai et al., "The Privacy Paradox and its Implications for Learning Analytics," March 23, 2020: 230–39.

8 Kukuh M. Raharjo et al., "Contribution of the Nonformal Education Labsite in Empowering Digital Technology-based Communities," *Atlantis Press,* 2023: 277–84.

Key Takeaways

Prateek Tripathi

The Digital Personal Data Protection Act, 2023[1] holds implications for the education sector. Passed after six years of consultations, the DPDP Act applies to all entities processing digitised personal data within India and to organisations outside India that process personal data to offer goods or services to data principals within India.[2]

India's diverse educational landscape[a] presents unique challenges in establishing digital privacy and data protection standards that are both comprehensive and adaptable. As the world's

[a] Due to the vastness and diversity of its landscape, education in India encompasses institutions of varying sizes, specialisations, and resources, both in academia and industry. There is a general lack of uniformity across educational institutions, ranging from large, well-funded universities in metropolitan areas to small, rural schools with limited infrastructure in impoverished localities.

second-largest e-learning market,[3] driven by increased internet penetration, reductions in internet prices, and hybrid learning models post-pandemic,[4] the DPDP Act will impact children's privacy in educational technology (edtech) services.

Challenges, Implementation, and Impact

Challenges

Edtech providers could face challenges in complying with Sections 9(1) and 9(3) of the DPDP Act, depending on how the subordinate legislation specifies the process for obtaining Verifiable Parental Consent (VPC). Obtaining parental consent[5] and creating user profiles may prove difficult, with VPC mechanisms potentially introducing new risks instead of mitigating them. Reports suggest that the government is considering using authorised agencies to approve tokenisation or DigiLocker for obtaining VPC. However, these intrusive, document-based processes could be disproportionate for edtech services operating parallel to the school system, raising privacy and cybersecurity concerns.[6,7] Furthermore, India's digital divide and low digital literacy levels raise concerns about the risk of parental consent being circumvented or not obtained meaningfully.[8,9]

The financial burden of upgrading IT infrastructure and implementing DPDP Act-compliant practices is substantial, particularly for underfunded institutions. Reliance on third-party vendors for Learning Management Systems (LMS) and cloud storage further complicates the establishment of comprehensive data-sharing protocols and restricts data access by roles and necessity. Resistance may also arise from staff and students accustomed to traditional data management practices. Furthermore, the DPDP Act's data-sharing restrictions could hinder academic collaboration, research, and essential activities such as placements, scholarships, and workshops.

Implementation

Assessing the suitability of VPC in the edtech context is crucial. In low-risk scenarios, alternatives that estimate a child's age without requiring parental intervention may be more appropriate.[10] Section 9(2) of the DPDP Act already prohibits the processing of children's data in ways that could harm their well-being. Additionally, clear protocols for obtaining parental consent and handling minor-specific data can ensure compliance while safeguarding vulnerable populations. Streamlined digital platforms for consent management and awareness campaigns for students and parents on the importance of data consent can further enhance protection efforts.

Cost-sharing models and government subsidies, combined with secure cloud services, can alleviate the financial burden on educational institutions, facilitating broader DPDP Act compliance. Establishing proper agreements with third-party vendors, implementing access controls, conducting regular vendor audits, and utilising data anonymisation

can effectively mitigate associated risks. Transition programs for staff and students, supported by institutional leaders advocating for DPDP Act's importance will be beneficial. Implementing time-limited and purpose-specific data access protocols can enhance collaboration, while flexible frameworks balancing data use and strict protection protocols can enhance effective data sharing.

Impact

Enhancing transparency and digital literacy for parents and children, implementing privacy-friendly-by-default systems, and enforcing strict data-sharing practices are essential for safeguarding children's interests.[11] Cost-sharing models and government support can alleviate financial burdens, facilitating broader compliance. Proper agreements, access controls, and specialised teams can effectively mitigate risks, streamline processes, and distribute workloads effectively. Change management strategies can address resistance, while rigorous vendor audits and detailed contracts can further enhance compliance. Grants and cloud solutions can address technological constraints, and data anonymisation with controlled access can maintain collaboration without compromising security. Flexible compliance frameworks can support educational activities, with pilot programs identifying best practices for broader implementation.

Implementation Recommendations

1. To adopt a proportionate, risk-based approach, the Central Government should consider exempting edtech providers from obtaining VPC under Section 9(1) and allow exceptions for behavioural tracking and monitoring under Section 9(3) when processing is solely for educational service provision. This exemption should be contingent on providers meeting specific standards to ensure adequate protection. Section 9(4) empowers the Central Government to impose certain conditions on these classes of data fiduciaries, enabling the establishment of higher standards. These may include data minimisation obligations, transparency requirements, individual rights such as data access, correction, and erasure, and additional accountability measures such as appointing a Data Protection Officer (DPO) and ensuring age-appropriate platform designs.[12]
2. Considering the widespread use of streaming platforms by Indian users for educational purposes, often offering free educational content,[b] the Central government should consider lowering the age for obtaining parental consent on streaming platforms that provide child-friendly, "verifiably safe" gateways for accessing educational material.

[b] Physics Wallah, a billion-dollar Indian edtech company, has over 12 million subscribers and 1500+ videos on YouTube.

3. Institutions should commence with a comprehensive data audit to identify compliance gaps, followed by the establishment of clear data governance policies aligned with the DPDP Act. Ongoing compliance requires continuous monitoring and regular reviews of data management practices.
4. Upgrading IT infrastructure with advanced security measures such as encryption and secure cloud storage is crucial for protecting sensitive data and building stakeholder trust.
5. Regular staff training on data minimisation, consent management, and secure data handling will enhance compliance. Additionally, creating collaborative platforms or committees involving educational institutions, technology providers, and regulatory bodies can foster innovative solutions and address shared challenges.
6. Collaborative innovation policies can promote partnerships between industry and universities to advance technology. Regulations for industry engagement should be established to maintain regulatory integrity.
7. Offering technology adoption incentives, such as tax breaks, can accelerate the implementation of secure data management systems. Capacity-building initiatives, including staff training programmes, are essential for effective data management.
8. Sector-specific support programmes tailored to address the unique challenges of the education sector can further strengthen the implementation of the legislation.

Conclusion

The enactment of the DPDP Act marks a watershed moment in India's data protection journey. While this shift is essential for safeguarding student data, enhancing stakeholder trust, and enabling data-driven decision-making, full compliance presents numerous challenges. However, these challenges are not insurmountable. By leveraging innovative solutions—such as cost-sharing models, digital consent platforms, and flexible compliance frameworks—institutions can effectively implement the Act while maintaining the agility necessary to foster educational innovation.

The law's comprehensive nature brings about a significant period of change for all stakeholders involved. Nevertheless, the gap between the law's enactment and the notification of subordinate legislation offers a valuable opportunity for regulators to implement the law in a manner that protects privacy and fosters sectoral growth.

Prateek Tripathi is Junior Fellow, Observer Research Foundation.

Endnotes

1 Ministry of Electronics and Information Technology, Government of India, "Digital Personal Data Protection Act 2023," https://www.meity.gov.in/content/digital-personal-data-protection-act-2023.

2 Raktima Roy and Gabriela Zanfir-Fortuna, "The Digital Personal Data Protection Act of India, Explained," *FPF Blog,* August 15, 2023, https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/

3 Aishwarya Anand, "India's Edtech Market Expected To Grow To $10 Billion By 2025," *CNBC TV 18,* April 12, 2023, https://www.cnbctv18.com/education/india-edtech-market-expected-to-grow-to-10-billion-by-2025-startups-unicorns-16391151.htm

4 Annapurna Roy, "How India Is Using the Internet," *The Economic Times,* March 10, 2024, https://economictimes.indiatimes.com/tech/technology/how-india-is-using-the-internet/articleshow/108354854.cms?from=mdr

5 "The State Of Play: Is Verifiable Parental Consent Fit For Purpose?," *FPF Blog,* June 2023, https://fpf.org/verifiable-parental-consent-the-state-of-play/

6 Soumyarendra Barik, "Aadhaar-based Consent For Children To Go Online Proposed In New Data Protection Rules," *The Indian Express,* December 17, 2023, https://indianexpress.com/article/india/aadhaar-based-consent-for-children-to-go-online-9071238/

7 "DigiLocker Bug Risked Info Of Over 38m Accounts," *HT Tech,* August 20, 2022, https://tech.hindustantimes.com/tech/news/digilocker-bug-risked-info-of-over-38m-accounts-71591106298225.html

8 Nistha Pandey, "NSSO survey |Only 31% Young Men In India Can Send Emails With Attachments," *CNBC TV 18,* March 27, 2023, https://www.cnbctv18.com/education/nsso-survey--only-31-young-men-in-india-can-send-emails-with-attachments-16275661.htm

9 Aparajita Bharti et al., "Navigating Children's Privacy and Parental Consent Under the DPDP Act 2023," *The Quantum Hub,* 2023, https://thequantumhub.com/wp-content/uploads/2023/11/TQH-YLAC-Childrens-Privacy-under-DPDP-Act-2023.pdf

10 Bharti et al., "Navigating Children's Privacy and Parental Consent Under the DPDP Act 2023."

11 Bailey Sanchez et al., ""Verifiably Safe" Processing Of Children's Personal Data Under the DPDPA 2023: A Catalogue Of Measures," *Future of Privacy Forum and the Dialogue,* 2023, https://fpf.org/wp-content/uploads/2023/11/Verifiably-safe-processing-of-childrens-personal-data-under-the-DPDPA-2023-A-Catalogue-of-Measures2.pdf

12 Sanchez et al, ""Verifiably safe" Processing of Children's Personal Data Under the DPDPA 2023: A Catalogue of Measures"

05

DATA PROCESSORS

Academic Perspective

Debayan Gupta

An Application Perspective

Nikhil Narendran

Key Takeaways

Shruti Shreya

Academic Perspective

Debayan Gupta

The Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant step by the Government of India towards regulating the use of personal data by both private and public entities.[1] Regulating data in a country as vast and complex as India is a monumental task: India is home to one-sixth of the world's population, with over a thousand languages, and a cryptographically secure biometric identity system that covers almost every citizen.[2,3,4]

While digitisation and data are seen as key pathways to improving the lives of Indian citizens, as a developing country with many large marginalised populations, India faces unique challenges. Any negative impacts of data misuse will likely be felt by those who can least afford them. Therefore, technical and regulatory efforts have been

underway to ensure that the digital revolution benefits everyone, rather than exacerbating inequality and exploitation.

Previous legislation in this area, such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, has become outdated. For instance, the IT Rules required companies collecting personal data to "obtain consent in writing through letter, fax, or email from the provider of the sensitive personal data or information regarding the purpose of usage before collection."[5] More importantly, from a data-processor perspective, the law mandated prior approval before any personal data could be disclosed or transferred to another party. The only exception was if the data transfer was "necessary for the performance of the lawful contract."[6] However, this seldom applies to cloud usage, where the primary drivers are cost savings, ease of maintenance, and guarantees of availability.[7]

The DPDP Act is reasonable in its division of responsibilities between data processors and data fiduciaries. However, in its current form, the law raises several issues for data processors, particularly regarding the withdrawal of consent, data processing for delivery services, and the rules surrounding the disclosure of processor identities. Despite these challenges, the DPDP Act's emphasis on consent and purpose limitations marks an important step towards effectively regulating this space.[8]

International Comparison

Countries worldwide have been working to regulate the use of personal and sensitive data. From the European Union's (EU) General Data Protection Regulation (GDPR) and Digital Services Act (DSA) to Argentina's Personal Data Protection Law and India's new DPDP Act, each framework presents its own set of rules.[9,10,11]

The Argentinian law mandates that personal data be collected only for specific, explicit, and legitimate purposes, prohibiting further processing unless it serves statistical, archival, or public interest research purposes.[12] It also enforces strict limitations on processing outdated or inaccurate data. Industries, in general, have struggled to navigate the complex interactions between these legal regimes across borders. For instance, an Indian service provider with clients in Germany or Argentina must comply with the strictest overlap of these countries' laws.

Given the economic dominance of the United States (US) and the EU, regulations in these regions tend to exert significant global influence, similar to the "California effect".[a,13] Firms operating solely within domestic markets will need to adapt, but

[a] The 'California effect' refers to a shift in regulatory standards that occurs due to stricter regulations in an important jurisdiction (state or country).

the majority of cloud platforms already function internationally, particularly in the EU and the US. This raises the question of whether Indian regulations such as the DPDP Act will meaningfully impact the behaviour of large firms. Many of the requirements in the GDPR, for instance, are already stricter than what the DPDP Act mandates. Ultimately, much will depend on how Indian authorities enforce the law and the specificity of audit requirements.

Challenges, Implementation, and Impact

Understanding the impact of the DPDP Act on data processors requires a nuanced, sector-specific approach. It is not practical to address all industries within this article, but some sectors present unique challenges, as outlined in the following paragraphs:

- **Delivery services:** A large portion of India's logistics infrastructure operates on the cloud, with many systems transitioning to microservice architectures. Under the current DPDP Act, certain common practices[b] may become illegal. Moreover, platforms like ONDC (Open Network for Digital Commerce) complicate matters by separating the cloud infrastructure of the ordering system from that of the manufacturer, provider, and delivery/logistics system.[14] Amending the law to allow for one-sided or delegated consent could resolve these issues and make such transactions lawful.
- **Healthcare:** This sector holds some of the most sensitive data, and with India moving towards large-scale, integrated digital health systems, data-processing systems like cloud infrastructure become essential.[15] While the DPDP Act avoids prescribing specific safeguards for handling such sensitive data, data processors managing healthcare data in India will face challenges in providing adequate security. Simply offering differential privacy is not enough; more sophisticated methods, like PAC privacy, will likely be necessary.[16,17]

  Given the wide disparity in equipment and resources across the country, much of India's health data will be uploaded from mobile devices to cloud servers for processing. Currently, the use of electronic health records is limited, and medical staff, who are already overburdened, often show reluctance to adopt new technologies.[18] However, advancements in telemedicine, diagnostic tools, personalised treatment plans, and communication with patients (many of whom speak different languages) could be revolutionary. These solutions, which do not require re-training or adding to staff workloads, are more likely

[b] E.g., a website which allows a user to order a delivery or gift for another. This might involve providing the latter's name, phone number, address, and even their date of birth (say, for a birthday present). The website thus becomes a data fiduciary for the recipient, without consent.

to be implemented quickly. Cloud-based data access and analytics can help overcome healthcare barriers, especially in rural areas. While healthcare chatbots may not be perfect, they often provide better care than no support at all. Moreover, there are enormous opportunities in areas like training, pathology, and data modeling. This is especially relevant for India and other developing countries, where high-quality data is scarce. During the COVID-19 pandemic, for example, cloud-based systems were vital for tasks ranging from disease tracking to predictive modeling and vaccine delivery.

- **Financial services and metadata:** Many data processors, such as cloud analytics providers, integrate data across multiple services by using metadata to draw inferences that would not be possible when data is collected from a single source. This practice is particularly common in the financial sector, where multiple UPI-based platforms rely on the data exhaust generated by user activity for profit.[19] These services do not necessarily use users' data directly but analyse patterns in metadata to make decisions about the data principals, as defined under the DPDP Act. This approach may cause legal issues under the DPDP Act, as the law explicitly covers data used to make decisions about individuals, although it does not directly address metadata.[20]

Upcoming rules and industry best practices must seek to establish a consensus on reasonable standards for reporting, deletion, and consent, especially when dealing with metadata processing. A natural tension exists between accountability and security, which cloud service providers need to navigate carefully. More advanced solutions, such as homomorphic encryption or secret-sharing, which allow for the processing of data without revealing them to the processor, are currently too slow for practical, large-scale applications.[21] As a result, data processors cannot claim the same level of security protections that have historically shielded end-to-end messaging platforms, making the need for robust, scalable security measures more urgent.

Beyond the clear emphasis on consent and purpose limitations, the DPDP Act embodies several fundamental principles. First, the law explicitly encompasses entities processing data belonging to Indian data principals, even if those entities are based outside India. Unlike the laxity of the EU-US Safe Harbor Framework and its stringent successor, the Privacy Shield, the DPDP Act aims to strike a careful balance between user privacy and industry feasibility.[22]

However, certain language in the law, particularly the requirement for explicit consent from the user or data principal for processing, may complicate some transactions. Additionally, since many data processors enable general computation,

it may be nearly impossible for them to determine when specific types of data traverse their systems, even while offering certain security guarantees to their customers.

Second, the DPDP Act attempts to differentiate between entities that handle sensitive data based on various individual risk factors, such as the volume and sensitivity of the personal data processed, as well as nation-state factors, including security and the risk to electoral democracy. Entities categorised under these criteria are subject to more stringent regulations and are required to undergo periodic audits.[23] Given the historical misuse of computational technology at both individual and nation-state levels, it is likely that all these risk factors will be thoroughly evaluated and tested in practice.[24,25]

Third, the regulations emphasise data deletion and grievance redressal, with explicit requirements for companies (data fiduciaries) to delete personal data upon request by data owners (data principals).[26] This includes the right to request a summary of collected data. However, provable deletion remains an unsolved challenge. The interconnected and interdependent nature of computational services has historically led to significant issues; for example, a recent code error from the security company CrowdStrike caused a global breakdown of Microsoft Windows systems.[27] This complexity is even more pronounced in cloud computing, where interlinked data flows across different geographies, security levels, and data types (both personal and non-personal), making it potentially unfeasible for data processors like cloud service providers to meet the law's deletion requirements effectively.

Implementation Recommendations

In the context of data processors, the following legislative amendments in three key areas would be required:

- **Reporting of data processors:** Many cloud providers may not wish (or even be able without unreasonable overhead) to reveal to every user exactly which sub-providers and servers they are using. This will especially affect smaller players, since larger, more vertically-integrated companies such as Amazon Web Services simply own much of their infrastructure outright, reducing their reporting requirements.
- **Standardising data-deletion protocols:** Cloud service providers must agree on and standardise protocols for the deletion of user data. The DPDP Act emphasises the withdrawal of user consent and the mandatory erasure of associated data. However, current data processors often maintain multiple backups, and the increasing use of microservice-based architectures has made the communication between different cloud systems more intricate. As provable deletion remains an unsolved challenge, it is essential to establish reasonable standard operating procedures (SOPs) to address this issue.

- **Limitations of consent in addressing privacy concerns:** Many privacy concerns in the digital ecosystem cannot be easily resolved through user consent alone. Therefore, service providers must take additional precautions to manage user data in ways that align with user expectations, recognising that these expectations can vary widely across different scenarios.

  Consider a scenario in which a citizen consents to share images of their retinas, believing that this data will be used solely for vision-related purposes. However, advanced analysis might reveal crucial details about their cardiovascular health, which could have serious implications, such as affecting insurance premiums. The individual may have no way of knowing that they are inadvertently sharing sensitive health information beyond their original intent.[28] In some cases, even the existence of such additional, sensitive insights may not be known at the time the data is first shared. As technology advances, this gap between what data users think they are sharing (x) and what is actually revealed (y) will only widen. This presents a massive challenge: How can ordinary individuals be expected to navigate the complexities of consent when they do not—and often cannot—know the full implications of what they are sharing?

  While the DPDP Act addresses these concerns by mandating that users be informed of and provide explicit consent for the purposes for which their data will be used, it does not adequately address the issue of combining user data with auxiliary data to infer additional insights. Furthermore, the law explicitly excludes state actors from most forms of liability. As a result, consent may not always serve as a practical or meaningful mechanism for determining the legality of data flows, especially as data processors and machine-learning platforms become more prevalent and sophisticated.

Conclusion

Despite being a lower-middle-income country, India has made remarkable strides in reducing poverty, with rates dropping from nearly 30 percent to just over 11 percent in the past decade.[29] A key driver of this progress has been the country's swift adoption of digital technologies, which have permeated even the remotest villages. However, gaps remain, particularly in crucial sectors like healthcare.[30] The combination of an ambitious, tech-savvy middle class, state-sponsored high-quality digital infrastructure, and concerted efforts to drive data-powered welfare initiatives for India's underserved population means that innovation in data-intensive technologies will continue to flourish. From startups to government agencies, entities are leveraging vast amounts of personal data to fuel advancements, with artificial intelligence (AI) being the prime example of this transformation.

In this landscape, it is vital to establish strong legislative frameworks such as the DPDP Act that can effectively protect individual privacy without stifling innovation. Balancing data protection with the needs of a rapidly evolving digital economy will be key to ensuring both economic growth and personal security.

The DPDP Act presents a crucial first step in regulating the use of digital personal data in India. In many ways, it surpasses comparable legislation from other regions, particularly in its focus on purpose limitation and informed consent.[31] By ensuring that consent is not merely a formality but an integral part of data processing, the DPDP Act sets a new standard for data privacy.

However, there are significant technical and practical challenges that the legislation must overcome, particularly around the withdrawal of consent and the extraterritorial transfer of data. The global nature of data processors, which often rely on geographically distributed servers and backups, could result in major hurdles in complying with these provisions. Additionally, as the legislation relies heavily on consent, there remains the issue that many users may not fully understand the downstream effects of sharing certain types of data. Consent, while necessary, may not always be sufficient to safeguard privacy, especially in a digital ecosystem as complex as the cloud. Therefore, there is a tangible need for amendments, potentially those emphasising purpose limitation, over consent in specific scenarios. Such reforms will require a massive interdisciplinary effort involving technology, law, and policy and are essential to ensuring that the DPDP Act remains both effective and feasible in the long run.[32]

It is essential that the Indian government maintains ongoing dialogue with industry, academia, and civil rights organisations to refine the DPDP Act. Like the national budget, the DPDP Act should be viewed as a dynamic framework that must evolve to address emerging technological challenges and societal needs. However, this adaptability must be balanced with clear, long-term principles that provide stability and continuity. This approach ensures that, while the legislation remains responsive to change, it also offers predictability for stakeholders, fostering trust and enabling informed planning for the future.

Debayan Gupta is Assistant Professor of Computer Science, Ashoka University, India.

Endnotes

[1] Ministry of Electronics and Information Technology, "Digital Data Protection Act," August 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

[2] Data Commons, "India," https://datacommons.org/place/country/IND?utm_%20medium=explore&mprop=count&popt=Person&hl=en#

[3] Ministry of Education, Government of India, "Indian Languages," https://www.education.gov.in/sites/up load_files/mhrd/files/upload_document/languagebr.pdf

[4] Pratyush Ranjan Tiwari et al., "India's "Aadhaar" Biometric ID: Structure, Security, and Vulnerabilities," in *International Conference on Financial Cryptography and Data Security* (Springer, 2022), 672–693.

[5] Ministry of Electronics and Information Technology, *Information Technology (Rea- sonable security practices and procedures and sensitive personal data or information) Rules, 2011*, April 2011, https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_ 0.pdf.

[6] India Code, "Already Registered," https://www.indiacode.nic.in/handle/123456789/1362/simple-search?query=The%20Information%20Technology%20(Reasonable%20Security%20Practices%20and%20Procedures%20and%20Sensitive%20Personal%20Data%20or%20Information)%20Rules,%202011.&searchradio=rules.

[7] Anol Bhattacherjee and Sang Cheol Park, "Why End-users Move To the cloud: A Migration-Theoretic Analysis," *European Journal of Information Systems* 23, no. 3 (2014): 357–372.

[8] Electronics and Information Technology, Digital Data Protection Act, 2.

[9] Paul Voigt and Axel Von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Cham: Springer International Publishing, 2017): 10–5555.

[10] Caroline Cauffman and Catalina Goanta, "A New Order: The Digital Services Act and Consumer Protection," *European Journal of Risk Regulation* 12, no. 4 (2021): 758–774.

[11] Arturo J Carrillo and Matías Jackson, "Follow The Leader? A Comparative Law Study Of The EU's General Data Protection Regulation's Impact in Latin America," *ICL Journal* 16, no. 2 (2022): 177–262.

[12] Arturo J Carrillo and Matías Jackson, "Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America," *ICL Journal* 16, no. 2, May 26, 2022: 177–262, https://doi.org/10.1515/icl-2021-0037.

[13] David Vogel, "Trading Up and Governing Across: Transnational Governance and Environ- mental Protection," *Journal of European public policy* 4, no. 4 (1997): 556–571.

[14] A. Shaji George and AS Hovan George, "Open Network for Digital Commerce (ONDC): Democratizing Digital Commerce and Curbing Digital Monopolies in India," *Partners Universal International Research Journal* 1, no. 2 (2022): 92–102.

[15] Sushila Paliwal et al., The Role of Ayushman Bharat Health Account (ABHA) In Tele- health: A New Frontier of Smart Healthcare Delivery in India, in *Proceedings of the Future Technologies Conference* (Springer, 2023), 388–406.

[16] Cynthia Dwork, "Differential Privacy," in *International Colloquium on Automata, Languages, and Programming* (Springer, 2006), 1–12.

17 Hanshen Xiao and Srinivas Devadas, "Pac Privacy: Automatic Privacy Measurement and Control of Data Processing," in *Annual International Cryptology Conference* (Springer, 2023), 611–644.

18 Sunil Kumar Srivastava, "Adoption of Electronic Health Records: A Roadmap for India," *Healthcare Informatics Research* 22, no. 4 (2016): 261.

19 Abhishek Kumar et al., "The Growth Trajectory Of UPI-Based Mobile Payments in India: Enablers and Inhibitors," *Indian Journal of finance and banking* 11, no. 1 (2022): 45–59.

20 Electronics and Information Technology, Digital Data Protection Act, 12.

21 Craig Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," in *Proceedings of the forty-first annual ACM symposium on Theory of computing* (2009), 169–178.

22 Newton C. Will and Carlos A. Maziero, "Intel Software Guard Extensions Applications: A Survey," *ACM Computing Surveys* 55, no. 14s (2023): 1–38.

23 Shufan Fei et al., "Security Vulnerabilities of SGX And Countermeasures: A Survey," *ACM Computing Surveys* (CSUR) 54, no. 6 (2021): 1–36.

24 Fabien Terpan, "EU-US Data Transfer From Safe Harbour To Privacy Shield: Back To Square One?," *European Papers-A Journal on Law and Integration* 2018, no. 3 (2019): 1045–1059.

25 Terpan, "EU-US Data Transfer From Safe Harbour To Privacy Shield: Back To Square One?"

26 Electronics and Information Technology, Digital Data Protection Act, 9.

27 Mika Westerlund, "The Emergence Of Deepfake Technology: A Review," *Technology Innovation Management Review* 9, no. 11 (2019).

28 Hal Berghel, "Malice Domestic: The Cambridge Analytica Dystopia," Computer 51, no. 5 (2018): 84–89.

29 Electronics and Information Technology, Digital Data Protection Act, 8.

30 A Shaji George, "When Trust Fails: Examining Systemic Risk in the Digital Economy From the 2024 CrowdStrike Outage," *Partners Universal Multidisciplinary Research Journal* 1, no. 2 (2024): 134–152.

31 João Viera Magalhães and Nick Couldry, "Giving by Taking Away: Big Tech, Data Colonial- ism and the Reconfiguration of Social Good," *International Journal of Communication* 15, 2021: 343–362.

32 David Scott, "India's Role in the South China Sea: Geopolitics and Geoeconomics In Play," *India Review* 12, no. 2 (2013): 51–69.

An Application Perspective

Nikhil Narendran

This chapter examines the impact of the Digital Personal Data Protection Act, 2023 (DPDP Act) on data processors. It focuses on how it affects two industry models: enterprise services (where providers serve enterprise customers),[a] and consumer services (where providers serve individual consumers).

The DPDP Act's applicability to an entity depends on its role in processing personal data.[b] A data fiduciary[c] bears the responsibility for complying with

---

a Some members of the cloud industry use the phrase 'enterprise cloud customers' to denote large business customers and exclude startups and micro, small, and medium enterprises (MSMEs). However, the term has been used in this article to denote all commercial entities, regardless of the size of the customer's business.

b Personal data is defined as "any data about an individual who is identifiable by or in relation to such data". Section 2(t), DPDP Act.

c A data fiduciary is defined as "any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data ". Section 2(i) of the DPDP Act.

specific obligations under the DPDP Act and must ensure that a data processor[d] contractually adheres to these obligations when processing personal data.

Applicability of the DPDP Act to Consumer-Facing Services

The impact of the DPDP Act on data processors' services will vary depending on the type of service. For instance, cloud providers offering consumer cloud services—such as email or online storage services via a software as a service (SaaS) model—interact directly with data principals.[e] In contrast, enterprise cloud service providers typically work with businesses that manage data principals. In the case of enterprise cloud services, it seems intuitive that the provider would function as a data processor. Similarly, consumer cloud service providers might appear to act as data processors. However, it is crucial to examine these assumptions in more detail.

Consumer services have evolved beyond offering simple, one-dimensional services. For example, an email service provider may not only facilitate sending emails but could also suggest responses by processing the contents of received emails. Similarly, when uploading documents to an online storage service, individual consumers make key decisions such as what to upload; in certain cases, the service provider may also make significant decisions by determining both the 'how' and the 'why' of personal data processing. For instance, it may process unique identifiers each time a document is accessed, assess how long a type of document has been in use, and improve service offerings based on such interaction data. In all these scenarios, where service providers determine the means ('how') and purposes ('why') of processing personal data, they will be classified as data fiduciaries under the DPDP Act.

The DPDP Act applies to data processors regardless of where their processing activities take place. This is because the Act governs the processing[f] of personal data either within India or outside India when offering goods or services to individuals in India.[1]

---

[d] A 'data processor' is defined as "any person who processes personal data on behalf of a Data Fiduciary"; Section 2(k), DPDP Act.

[e] A 'data principal' is defined as "the individual to whom the personal data relates and where such individual is— (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf"; Section 2(j), DPDP Act.

[f] 'Processing' in relation to personal data is defined as "a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction"; Section 2(x), DPDP Act.

Consumer-facing data processors must comply with obligations applicable to data fiduciaries under the DPDP Act, including providing notice and obtaining consent. The compliance requirements, which are detailed in Annexure 1, include implementing reasonable security safeguards to prevent personal data breaches and notifying the Data Protection Board and affected data principals of any breach. Failure to meet these obligations could lead to significant penalties, ranging from ~US$23 million to ~US$30 million, with other contraventions (e.g., not providing notice or obtaining consent) attracting fines of up to US$6 million. While penalties are expected to apply only to significant contraventions, the DPDP Act does not define what constitutes a "significant" breach. Therefore, data processors must carefully assess their role in handling personal data and ensure compliance with all relevant measures.

The government may designate certain data fiduciaries or classes of data fiduciaries as "significant" data fiduciaries[g] based on factors such as the volume and sensitivity of personal data processed. The obligations applicable to significant data fiduciaries, outlined in Annexure 1, include additional compliance requirements. Although no clear intent is evident at present, it is possible that the government could classify some consumer-facing data processors as significant data fiduciaries, subjecting them to stricter compliance standards.

Applicability to Enterprise Service Providers

For most enterprise services—where an organisation is the end customer using an array of services from a provider—the service provider is generally considered a Data Processor. In such situations, the enterprise customer typically determines the purpose and means of processing personal data, making them the data fiduciary.

In cases where enterprise services are treated as data processors, regardless of their location, the DPDP Act does not impose direct obligations on them. However, the data fiduciary (the enterprise customer) must contractually ensure that the data processor adheres to the obligations required of the data fiduciary under the DPDP Act, such as implementing reasonable security safeguards to prevent personal data breaches.

There is an argument that the DPDP Act may not apply to offshore enterprise

---

g A 'significant data fiduciary' is defined as any "Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10"; Section 2(z), DPDP Act. Section 10(1) empowers the Central Government to notify significant data fiduciaries based on its assessment of "relevant factors", including: "(a) the volume and sensitivity of personal data processed; (b) risk to the rights of Data Principal; (c) potential impact on the sovereignty and integrity of India; (d) risk to electoral democracy; (e) security of the State; and (f) public order."

service providers offering services to enterprise customers in India. Section 3(b) of the Act implies that it applies to offshore processing only when it involves providing services directly to data principals in India. Since enterprise service providers typically do not offer services directly to end users, it is arguable that such processing falls outside the scope of the DPDP Act.

When personal data is processed in India, such as when data processors collect data in India or host data centres there, the question of DPDP Act applicability does not arise. This is because the processing activity falls within the Act's scope since it occurs in India.

Although the Act does not impose direct obligations on data processors, they remain subject to information requests from the government regardless of their location. The government has the authority to issue information requests related to the DPDP Act to any intermediary, which includes individuals or entities providing services regarding electronic records.

Determining the role of a data processor is not straightforward and must be assessed at each instance. For example, an enterprise service provider might also be classified as a data fiduciary for the personal data it manages on behalf of its enterprise customer. If the provider analyses the personal data it processes—such as how end users interact with specific tools—to enhance its service offerings, it qualifies as a data fiduciary for that data. Moreover, even if an enterprise service provider acts as a data processor regarding end users' personal data, it may still be a data fiduciary regarding any business contact information (e.g., customer representatives' details) that it processes for its enterprise customers. The DPDP Act also recognises a co-fiduciary model, where multiple data fiduciaries collaborate to determine the means and purposes of processing. Thus, while the enterprise service provider will often act as a data processor, it will be regarded as a co-fiduciary if it determines the means and purposes of processing certain personal data. In such instances, the obligations outlined in Annexure 1 will apply to these providers, along with the associated penalties for non-compliance.

Understanding Means and Purposes

The DPDP Act does not explicitly define the terms 'purpose' or 'means'. In the absence of such clarity, it is prudent to refer to the General Data Protection Regulation (GDPR), which uses similar definitions for 'data controllers' (similar to data fiduciaries in the DPDP Act) and 'data processors'. Under the GDPR, determining the purpose and means of processing personal data involves answering the questions of why and how personal data is processed.[2]

In its *Guidelines 07/2020 on the concepts of controller and processor under the GDPR,* the European Data Protection Board clarifies that a data controller is responsible for determining the why and how of personal data processing.

However, certain "non-essential means" (i.e., non-essential hows) can be delegated to a data processor. This delegation of non-essential means does not cause the processors to be classified as data fiduciaries.[3]

The European Data Protection Board clarifies that "'[e]ssential means' are means that are closely linked to the purpose and the scope of the processing."[4] For instance, deciding which personal data to process and determining how long to retain it counts as "essential means".[5] Consequently, the entity that makes such a determination qualifies as a controller (the GDPR equivalent of a data fiduciary) if it also decides the purpose of processing. In contrast, the European Data Protection Board clarifies that non-essential means relate to "practical aspects of implementation, such as the choice of a particular type of hardware or software or the detailed security measures that may be left to the processor."[6] Crucially, deciding the purpose and means are conjunctive requirements: both the why and the how must be satisfied for an entity to be treated as a data fiduciary.

Certain service providers, especially in the SaaS segment, offer several standardised products. While the SaaS provider defines the preliminary aspects of the product, as long as the customer (i.e., the enterprise customer) decides the essential means—such as when, where, and whether to use the product, including what personal data to process—the SaaS provider can assume the role of a data processor. Similarly, a data processor's decisions regarding how it processes personal data (e.g., the security protocols it deploys) do not make it a data fiduciary unless it also determines the purposes behind that processing. For example, if a service provider uses end-user details to market its offerings directly to those end users, it is acting independently rather than on behalf of the enterprise customer.

While an enterprise service provider will typically act as a data processor, some scenarios may require it to function as a co-fiduciary. In such cases, the service provider must obtain consent from the data principal and comply with all necessary obligations applicable to a data fiduciary under the DPDP Act. This approach aligns with the Working Party Opinion regarding SWIFT.[7] In that instance, the Working Party evaluated a series of data transfers made by SWIFT to offshore operational centers in the United States (US) and the provision of access to certain personal data to US law enforcement authorities. The Working Party opined that such transfers and access were "incompatible with the original, commercial-only purpose for which personal data [had] been collected," noting that "SWIFT ha[d] not pointed this purpose out…to the users of its services [or] to any data protection supervisory authority."[8] Consequently, the Working Party called on SWIFT to take the necessary measures to comply with its obligations under Belgian data protection law when it acted as a controller.[9]

Enterprise Service Providers as Data Processors

When the enterprise service provider acts as a data processor, the enterprise customer, as the data fiduciary, must engage the provider through a contract.[10] This contract must clearly outline the roles and responsibilities of both parties regarding personal data processing. It is crucial that these contracts not only define the responsibilities by nomenclature but also substantively delineate roles and responsibilities.

While the enterprise service provider can manage non-essential means of processing personal data, the enterprise customer must ensure that these protocols are reasonable and appropriate for the personal data being handled. The enterprise service provider should also bear contractual responsibility for actions it takes on behalf of the data fiduciary. It cannot independently initiate a new processing activity outside the scope of the contract. Additionally, it must delete personal data upon the customer's instruction, subject to regulatory retention requirements, or transfer such controls to the customer.

An enterprise customer's control over data processing is enabled not only through contracts but also through technological measures. In most cases, it is essential for the customer to retain control over the personal data, including enabling end users' rights to access, correct, and delete their personal data.[h]

An enterprise customer remains responsible for the data-processing activities undertaken by a data processor, even if a contract states otherwise.[11] Therefore, enterprise customers must ensure that the implemented data-processing service complies with the requirements under the DPDP Act, including the obligations for notice and consent in consent-based processing and handling erasure requests. When the service provider operates outside India (i.e., where processing occurs outside India), the customer should include contractual provisions to ensure sufficient cooperation with the Indian data protection authority (i.e., the Data Protection Board) regarding any potential enforcement actions.

While contractual indemnity may help pass on contractual risks, it will not serve as a free pass regarding

---

[h] Privacy principles such as the right to access, and the right to have personal data erased at the option of the Data Principal, are baked into the DPDPA as statutory rights provided to Data Principals. Enabling the availability and exercise of such rights is thus pivotal to any Data Fiduciary's compliance with the DPDPA. As the Data Fiduciary may pass on such obligations to the Data Processor contractually, it is imperative that cloud service providers in their capacity as processors build in such processes, too.

regulatory enforcement or associated public relations risks. Enterprise service providers must understand that their responsibilities extend beyond merely servicing contractual penalties. The Data Protection Board, in performing its functions under the DPDP Act, possesses the powers of a civil court. This includes the authority to summon and enforce the attendance of any person, examine them under oath, receive evidence, require the discovery and production of documents, and inspect any data or records.[12] Accordingly, enforcing the DPDP Act regarding an enterprise customer will also require the service provider to cooperate with the Data Protection Board's inquiry proceedings.

Compliance with DPDP Act by Design

Regardless of the role that a service provider performs, ensuring compliance with the DPDP Act during the processing of personal data is essential. Although the enterprise customer bears the statutory responsibility for complying with the DPDP Act in enterprise services, data processors as a whole must foster an environment of trust for their entire customer base. To achieve this trust, data processors must align with the privacy and data-protection principles enshrined in the DPDP Act.

Data processors should use this intervening period to examine how they design their services. They must identify how personal data flows into their systems and the protocols surrounding its management and protection. Additionally, providers should ensure that their customers—both end users and enterprise customers—have adequate tools to comply with the DPDP Act. This includes tools that enable swift identification and erasure of personal data upon a data principal's request as well as measures to trigger notification protocols for personal data breaches.

Implementing these strategies will not only drive further adoption of different forms of data processing services in India but also significantly enhance trust among both government and private-sector stakeholders.

Annexure 1: Obligations of Data Fiduciaries and Significant Data Fiduciaries

A. Obligations Applicable to All Data Fiduciaries

1. **Process Personal Data Lawfully:** Only process personal data for lawful purposes, based on either consent or legitimate use.[13]
2. **Obtain Verifiable Consent:** When handling the personal data of protected classes (i.e., children and persons with disabilities who have a lawful guardian), obtain verifiable consent in the manner prescribed by the government.[14]
3. **Appoint Data Processors:** If required, appoint data processors under a contract and ensure that they handle personal data in accordance with the DPDP Act.[15]
4. **Implement a Grievance Redressal Mechanism:** Establish an effective grievance redressal mechanism.[16]

5. **Designate a Point of Contact:** Designate a point of contact to handle grievances from data principals regarding their personal data, and publish this information as prescribed.[17]
6. **Protect Personal Data:** Ensure the protection of personal data in your possession or control (including where a data processor undertakes processing), and institute reasonable security safeguards to prevent data breaches.[18]
7. **Report Data Breaches:** Report personal data breaches to the Data Protection Board (the enforcement authority to be established under the DPDP Act) and to affected data principals in the manner prescribed by the Indian government.[19]
8. **Implement Technical and Organisational Measures:** Implement appropriate technical and organisational measures to ensure effective observance of the DPDPA.[20]
9. **Ensure Data Accuracy:** Ensure the completeness, accuracy, and consistency of personal data being processed, especially if it will be used to make decisions about a data principal or shared with another data fiduciary.[21]
10. **Erase Personal Data:** Erase personal data unless retention is necessary for compliance with any law, when a data principal withdraws consent, or as soon as it is reasonable to assume that the specified purpose of processing is no longer being served. Data fiduciaries must also ensure their data processor erases any personal data made available to it.[22]
11. **Enable Data Principals to Exercise Their Rights:** Enable data principals to exercise their statutorily provided rights regarding their personal data, including the following: the right to access a summary of the personal data processed and to know whom it is shared with;[23] the right to seek erasure of personal data; the right to have personal information updated, corrected, or completed;[24] the right to nominate another person to act on behalf of the data principal in the event of death or incapacity;[25] and the right to readily available means of grievance redressal.[26]

B. Obligations Applicable to Significant Data Fiduciaries

1. **Appoint a Data Protection Officer:** Appoint a Data Protection Officer[i] to represent them under the provisions of the Act. The Data Protection Officer must be based in India; be an individual responsible to the Board of Directors or a similar governing body of the Significant Data Fiduciary; and serve as the point of contact for the grievance redressal mechanism under the DPDP Act.[27]

[i] A Data Protection Officer is defined as "an individual appointed by the Significant Data Fiduciary under clause (a) of sub-section (2) of section 10"; Section 2(l), DPDP Act.

2. **Appoint an Independent Data Auditor:** Appoint an independent data auditor to evaluate the Significant Data Fiduciary's compliance with the DPDPA[28] and undertake periodic audits.[29]
3. **Undertake Periodic Data Protection Impact Assessments:** Conduct periodic Data Protection Impact Assessments, describing the rights of data principals, the purpose of processing their personal data, an assessment and management of the risks to data principals' rights, and any other matters prescribed by the Central Government.[30]
4. **Implement Additional Measures:** Undertake any other measures consistent with the DPDP Act, as prescribed by the Central Government.[31]

Nikhil Narendran is a lawyer who specialises in the interplay between technology, law, commerce, and human lives.

Endnotes

1 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 3," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

2 The European Commission, "What Is a Data Controller Or a Processor?," *Rules for Business and Organisations*, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_en

3 The European Data Protection Board, "Purposes and Means," Guidelines 07/2020 on the concepts of controller and processor in the GDPR, July 7, 2021: 14.

4 The European Data Protection Board, Guidelines, Page 15.

5 The European Data Protection Board, Guidelines, Page 15.

6 The European Data Protection Board, Guidelines, Page 15.

7 Article 29 Data Protection Working Party, *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, adopted on 22 November 2006.

8 Working Party Opinion, page 15.

9 Working Party Opinion, page 27.

10 Section 8(2), DPDPA mandates that "A Data Fiduciary may engage, appoint, use or otherwise involve a Data Processor to process personal data on its behalf for any activity related to offering of goods or services to Data Principals only under a valid contract".

11 Section 8(1), DPDPA clarifies that "[a] Data Fiduciary shall, irrespective of any agreement to the contrary or failure of a Data Principal to carry out the duties provided under this Act, be responsible for complying with the provisions of this Act and the rules made thereunder in respect of any processing undertaken by it or on its behalf by a Data Processor."

12 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 28(7)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

13 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 4," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

14 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 9(1)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

15 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 8(1)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

16 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 8(10)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

17 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 8(9)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

18 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 8(5)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

19 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 8(6)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

20 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 8(4)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

21 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 8(3)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

22 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 8(7)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

23 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 11," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

24 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 12," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

25 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 14," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

26 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 13," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

27 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 10(2)(a)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

28 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 10(2)(b)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

29 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 10(2)(c)(ii)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

30 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 10(2)(c)(i)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

31 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023-Section 10(2)(c)(iii)," https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

Key Takeaways

Shruti Shreya

The Digital Personal Data Protection Act, 2023 (DPDP Act) has transformed India's data protection landscape, significantly impacting data processors. Although the Act primarily targets data fiduciaries, it imposes essential indirect obligations on data processors to ensure adherence to data-protection standards. This article examines the evolving role of data processors, highlighting their expanding responsibilities under the DPDP Act. It discusses the shift towards a co-fiduciary model in specific contexts and data processors' engagement with emerging challenges, such as cross-border data transfers and AI-driven data processing. In doing so, it underscores the increasing accountability of data processors and draws comparisons with global data-protection frameworks.

The Expanding Accountability of Data Processors

The DPDP Act defines 'data processors' as entities that process personal data on behalf of data fiduciaries (Section 2(14)).[1] While the Act does not directly impose obligations on data processors like it does on data fiduciaries, it establishes a framework of accountability that requires data processors to adhere to security standards and safeguard personal data. Section 10(3) mandates that data fiduciaries ensure that data processors comply with appropriate security measures through binding contracts.[2]

This contractual arrangement elevates the responsibilities of data processors from mere executors of tasks to active participants in ensuring the integrity and confidentiality of personal data. Data processors must implement stringent security protocols to protect the data they process, especially in the event of a data breach.[3] Although the Act does not directly impose a breach notification obligation on data processors, their cooperation with data fiduciaries remains essential for the timely reporting of breaches to the Data Protection Board, as required under Section 9(5). This growing interdependence highlights the evolving role of data processors in maintaining data-protection compliance.

In global frameworks like the European Union's General Data Protection Regulation (GDPR), data processors have direct obligations such as maintaining records of processing activities and ensuring that data-protection measures are in place. Although the DPDP Act does not yet impose similar direct obligations on data processors, it expects them to engage proactively in security and compliance efforts. This expectation indicates a global shift towards shared accountability in data protection.

The Co-Fiduciary Model: Joint Responsibility in Data Processing

The DPDP Act introduces the possibility of joint responsibility between data fiduciaries and data processors, especially in scenarios where data processors exert significant control over the means of processing. Section 2(13) of the DPDP Act defines a 'data fiduciary' as any entity that determines the purposes and means of data processing, either alone or with others.[4] This definition creates the possibility of a co-fiduciary model, especially in complex data-processing arrangements such as cloud services, where data processors can influence key aspects of data handling.

In such cases, where data processors determine aspects like the retention period or security measures for personal data, their role extends beyond mere data processing. While the DPDP Act primarily holds data fiduciaries accountable, shared responsibility arises when data processors influence how data is processed. This co-fiduciary arrangement may require data processors to meet additional compliance obligations, such as obtaining

consent from data principals or ensuring transparency in their data-processing activities.

A parallel instance is the GDPR's concept of joint controllers, where two or more entities determine the purposes and means of processing personal data.[5] The GDPR explicitly recognises joint responsibility and sets clear guidelines for identifying which parties are liable for ensuring compliance.[6] Although the DPDP Act does not explicitly codify such a model, the framework it establishes suggests that joint responsibility could arise in scenarios where data processors assume significant decision-making roles in data-processing activities.

Navigating Cross-Border Data Transfers

A key feature of the DPDP Act regulates cross-border data transfers.[7] Section 17 of the legislation allows the Central Government to designate specific jurisdictions as trusted for cross-border transfers, provided they have adequate safeguards in place.[8] Data processors, particularly in the cloud services industry, must navigate this complex regulatory environment when processing personal data for Indian data fiduciaries using global data centres.

Although the Act places the primary responsibility for cross-border transfers on data fiduciaries, data processors play an integral role in ensuring compliance with these provisions. Data processors managing cloud infrastructures must implement appropriate safeguards, such as data encryption and secure transfer protocols, to prevent unauthorised access during cross-border data flows. They must also ensure that their contractual agreements with data fiduciaries include clauses addressing the legal requirements for international data transfers, as outlined in Section 10(3) of the DPDP Act.

The GDPR, in contrast, provides detailed guidance on cross-border data transfers through mechanisms such as adequacy decisions and Standard Contractual Clauses (SCCs).[9] These frameworks ensure that personal data transferred outside the European Economic Area receives similar levels of protection.[10] Data processors under the GDPR bear direct responsibility for ensuring that their international data transfers comply with these standards. Similarly, data processors under the DPDP Act must be mindful of the evolving list of trusted jurisdictions and collaborate closely with data fiduciaries to maintain compliance with both Indian and international data-protection standards.

Data Processors in the Age of AI and Automation

The rise of artificial intelligence (AI) and automated data processing introduces unique challenges for data processors under the DPDP Act. AI systems typically process vast amounts of personal data, raising concerns about fairness, transparency, and accountability. Data processors involved in developing AI algorithms must ensure that their processing practices align with the

principles of purpose limitation and data minimisation, as outlined in Section 6 of the DPDP Act.[11]

In AI-driven systems, data processors often play a dual role, processing data on behalf of data fiduciaries and developing the algorithms that analyse the data.[12] This dual role gives them influence over the methods of data processing, potentially elevating their role to that of a co-fiduciary.[13] The DPDP Act's requirement to obtain consent from data principals before processing their personal data (Section 7)[14] applies equally to AI-driven data processing, making transparency about data usage and the ability to rectify or erase personal data critical.[15]

The global regulatory landscape is evolving to address these challenges. For instance, the European Union's proposed Artificial Intelligence Act introduces specific obligations for developers and processors of high-risk AI systems,[16] focusing on transparency, fairness, and accountability in AI-based decision-making.[17] In India, although the DPDP Act does not yet include AI-specific provisions, data processors involved in AI technologies must ensure that their systems align with the broader data-protection principles of the Act, especially in sectors like healthcare, finance, and education, where AI is increasingly being deployed.

Conclusion

The DPDP Act marks a new chapter in the development of India's data-protection landscape, expanding the role of data processors beyond merely executing instructions from data fiduciaries. Data processors are now expected to implement proactive data-protection measures, comply with data localisation requirements, and take responsibility for securing cross-border data transfers. The growing potential for joint responsibility, especially when data processors control aspects of data processing, further highlights the evolving nature of their role. Compared to global frameworks like the GDPR, the DPDP Act places indirect but substantial obligations on data processors, requiring close collaboration with data fiduciaries to ensure compliance. With emerging technologies such as AI and automation reshaping data processing, data processors must adopt a forward-thinking approach, designing systems that prioritise privacy and data protection. In doing so, they will not only meet their legal obligations but also help create a more secure and trustworthy digital ecosystem in India.

Shruti Shreya is former Senior Programme Manager, Platform Regulation and Gender and Tech, The Dialogue.

Endnotes

1 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act 2023, Section 2(14)," 2023

2 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act 2023, Section 10(3)," 2023

3 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act 2023, Section 9(5)," 2023; General Data Protection Regulation, "Article 32- Security of processing," https://gdpr-info.eu/art-32-gdpr/

4 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act 2023, Section 2(13)," 2023

5 Dimitra Kamarinou et al., "Responsibilities of Controllers and Processors of Personal Data in Clouds," in *Cloud Computing Law,* ed. Christopher Millard(Oxford: Oxford Academic, 2021), https://doi.org/10.1093/oso/9780198716662.003.0009.

6 General Data Protection Regulation, "Article 26- Joint controllers," https://gdpr-info.eu/art-26-gdpr/

7 Anirudh Burman, "Understanding India's New Data Protection Law," Carnegie Endowment for International Peace, 2023, https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law.

8 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act 2023-Section 17," 2023.

9 General Data Protection Regulation, "Articles 44–50-Transfers of personal data to third countries or international organizations," https://gdpr-info.eu/

10 Daniel Perray, "Post- 'Schrems II': Can EU Regulators Set Aside a Risk-Based Approach for Conducting Transfer Impact Assessments?," IAPP, 2022, https://iapp.org/news/a/post-schrems-ii-can-eu-regulators-set-aside-a-risk-based-approach-for-conducting-transfer-impact-assessments.

11 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act 2023, Section 6," 2023

12 General Data Protection Regulation, "Recital 78-Appropriate safeguards in the context of personal data processing by design," https://gdpr-info.eu/recitals/

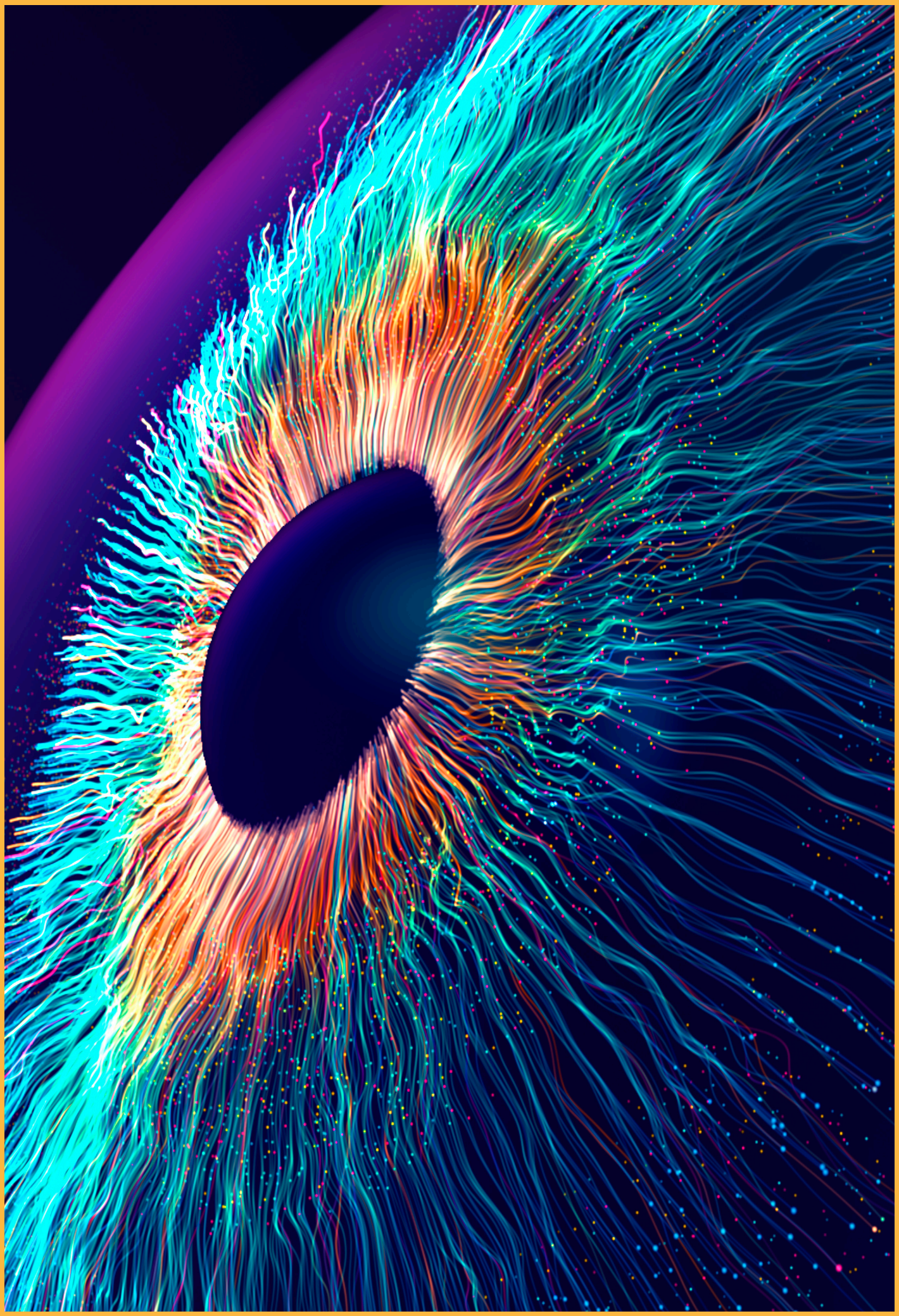
13 Harini Singh, "Navigating AI Regulation: A Comparative Analysis of EU and Lessons for India," INDIAai, February 19, 2024, https://indiaai.gov.in/article/navigating-ai-regulation-a-comparative-analysis-of-eu-and-lesson-for-india.

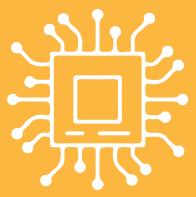
14 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act 2023, Section 7," 2023

15 "What's New? | India," in *Global Data Privacy and Cybersecurity Handbook* (Baker McKenzie Resource Hub, December 22, 2023), https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/asia-pacific/india/topics/whats-new.

16 Giovanni Sartor, "The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence," European Parliamentary Research Service, 2020, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

17 European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act)*, COM/2021/206 final.





06

EMERGING TECHNOLOGIES

Potential Impact of the DPDP Act on Emerging A.I. Technologies

Pranav Bhaskar Tiwari

Potential Impact of the DPDP Act on Emerging A.I. Technologies

Pranav Bhaskar Tiwari

From education and finance to politics and the judiciary, artificial intelligence (AI) is creating novel prospects across sectors, weaving into the social fabric of modern societies. However, this transformation brings complex legal challenges, particularly concerning data protection. In India, the Digital Personal Data Protection (DPDP) Act of 2023[1] places explicit obligations[2] on entities that collect, store, or process personal data,[3] including AI companies. Since AI systems rely on vast amounts of data for training and operational efficiency, AI-enabled businesses must navigate the provisions of the DPDP Act with care. This chapter analyses how the DPDP Act impacts the use of AI technologies, focusing on compliance issues, risks, and best practices for AI companies.

AI systems typically train on large datasets, including user-generated content from social media,[4] customer data,[5] information collected from web scraping,[6] public data, and proprietary data.[7] These data-sourcing methods raise potential infringements of copyright,[8] concerns of data protection,[9] and issues regarding *sui generis* database rights.[10]

Compliance with the core obligation of consent envisaged under the DPDP Act[11] requires the data fiduciary to furnish clear notice to users in English and all official Indian languages explaining the purpose of data collection and processing.[12] Consent must be free, specific, informed, unconditional, unambiguous, and obtained via affirmative action. When engaging with the personal data of minors or persons with disabilities, verifiable consent of their parents or lawful guardians is essential.[13] Enterprises processing pre-existing data must furnish fresh notice as soon as reasonably possible,[14] and obtain informed consent if not sought earlier.

Compliance Challenges for AI Systems

AI-enabled businesses functioning as data fiduciaries must fulfil essential requirements under the DPDP Act.[15] Compliance with the legislation entails cost of implementing robust safeguards along with technical compliance to avert breaches,[16] restricting data processing to its pre-defined purpose,[17] preserving data accuracy,[18] and purging personal data when it is no longer required.[19] Non-compliance not only leads to legal and financial penalties but a single breach or mishap can diminish consumer trust and institutional reputation. This would directly impact the sustainability and scalability of AI-enabled businesses.

Obligations are more stringent for AI organisations classified as significant data fiduciaries (SDF) due to the volume or sensitivity of data processed.[20] These encompass the appointment of an India-based data protection officer (DPO),[21] execution of data protection impact assessments (DPIAs),[22] conducting regular audits of data processing,[23] implementation of sophisticated security measures, and compliance with government directives.[24]

Notably, businesses retain accountability even when incorporating third-party AI systems.[25] In these instances, contracts must guarantee that third parties comply with the DPDP Act's stipulations. If a third party dictates the methods and objectives of processing, it may assume the responsibilities of a data fiduciary. AI businesses must contractually organise such interactions to mitigate any liabilities.

AI companies training models on anonymised data must exercise caution too. While the DPDP Act exempts anonymised data from compliance requirements, obligations under the Act may be triggered if the data is de-anonymised. AI developers must deploy state-of-the-art anonymisation techniques to mitigate this risk.

Exemptions and Restrictions

Certain activities are excluded from the rigours of the DPDP Act, primarily when AI is employed for statistical, research, or archiving purposes, as long as the data is not utilised for decision-making that impacts data principals.[26] Additionally, AI utilised for law enforcement purposes, including crime prevention or prosecution, is exempt and its use is contingent upon implementing adequate security measures to avert data breaches.[27]

The Act, however, restricts some high-risk practices unless exempted by a government authority, including the behavioural surveillance of minors and targeted advertising.[28] AI businesses involved in such activities must guarantee that their operations adhere to these limitations, particularly considering the increasing emphasis on safeguarding vulnerable populations from data misuse.

Best Practices for AI Companies

As AI companies address the intricacies of the DPDP Act, implementing best practices is crucial for ensuring compliance and mitigating risks. The following points outline some practical measures to consider.

a. **Consent mechanisms:** AI companies must ensure users understand how their data will be processed.
b. **Anonymisation of training data:** Ensuring that data is anonymised or pseudonymised mitigates compliance risks. AI enterprises must ensure that AI models cannot re-identify anonymised data, as this would trigger the obligations envisaged in the DPDPA.
c. **Contractual safeguards:** Companies must establish robust contractual obligations to ensure adherence to the DPDP Act when integrating third-party AI systems. This involves mandating that third-party vendors comply with security and consent standards.
d. **Audits and impact assessments:** Regular audits and DPIAs will enable AI companies to identify potential risks and maintain compliance with data protection obligations.
e. **Opt-out options:** AI companies utilising user-generated prompts or feedback for model training must ensure that users can opt out of such data usage, adhering to international best practices, including those outlined by the European Data Protection Board.[29] AI companies must further assume that users will likely share personal data in their prompts. Accordingly, the company must anonymise the data before using it for training.

Pranav Bhaskar Tiwari is Senior Programme Manager, Platform Regulation and Gender and Tech, The Dialogue.

Endnotes

1 Digital Personal Data Protection Act, Act No. 22 of 2023 (2023) (hereinafter referred to as DPDPA).

2 Two conditions have been imposed on processing the personal data of an individual by entities, namely, the 'consent' of the individual, or otherwise, 'legitimate reasons'; section 4(1), DPDPA.

3 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 2(x)," 2023.

4 A. Jaiswal et al., "Ethics of the Use of Social Media As Training Data For AI Models Used For Digital Phenotyping," *JMIR Formative Research* 8, 2024, https://formative.jmir.org/2024/1/e59794/.

5 Prakruti Mishra, "LinkedIn Trains Generative AI Models On User Data, Offers Opt-Out Option," *Business Standard*, September 19, 2024, https://www.business-standard.com/technology/tech-news/linkedin-trains-generative-ai-models-on-user-data-offers-opt-out-option-124091900428_1.html.

6 Lee Tiedrich, comment on "The AI Data Scraping Challenge: How Can We Proceed Responsibly?," The OECD.AI Policy Observatory, comment posted on March 5, 2024, https://oecd.ai/en/wonk/data-scraping-responsibly.

7 Tom Davenport and Maryam Alavi, "How To Train Generative AI Using Your Company's Data," *Harvard Business Review*, July 6, 2023, https://hbr.org/2023/07/how-to-train-generative-ai-using-your-companys-data.

8 New York Times Company v. Microsoft Corp., et al, Case No. 1:23-cv-11195 (S.D.N.Y., 2023).

9 "Guidance On AI and Data Protection," UK Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/.

10 Apar Gupta, "Protection Of Databases In India and Sui Generis Protection," *Journal of Intellectual Property Law & Practice*, no. 2 (2007), https://academic.oup.com/jiplp/article-abstract/2/8/553/845160?redirectedFrom=fulltext.

11 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 6(1)," 2023.

12 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 5(3)," 2023.

13 A minor is defined as an "*individual who has not completed the age of eighteen years*"; section 2(f), DPDPA. Provisions for processing the personal data of a minor, or a differently abled person are enshrined in section 9, DPDPA. The special conditions imposed with respect to these stakeholders are taking the consent of their guardian, declining to process their data in case its consequences are detrimental to the stakeholder and to refrain from monitoring them for targeted advertisements.

14 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 5(2)(a)," 2023.

15 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 8," 2023.

16 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 8(5)," 2023.

17 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 5(2)(i)," 2023.

18 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 12(2)(a)," 2023.

19 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-Section 8(7)(a)," 2023.

20 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 2(z)," 2023.

21 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 2(l)," 2023.

22 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 10 (2)(c)(i)," 2023.

23 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 10 (2)(c)(ii)," 2023.

24 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 10(2)(c)(iii)," 2023.

25 McCoy et al., "Ethical Responsibilities for Companies That Process Personal Data" *The American Journal of Bioethics*, no. 11(2023), https://doi.org/10.1080/15265161.2023.2209535

26 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 17(2)(b)," 2023.

27 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 17(1)(c)," 2023.

28 Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act-section 9(3)," 2023.

29 EDPB, *Report of the work undertaken by the ChatGPT Taskforce*, Brussels, European Data Protection Board, 2024, https://www.edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-chatgpt-taskforce_en.

CONCLUSION

Kamesh Shekar

As India moves forward with implementing the Digital Personal Data Protection (DPDP) Act 2023, it is essential to understand its sectoral nuances to facilitate a seamless transition towards privacy compliance and operationalisation of data protection principles and standards. As a contribution to the process, this compendium has gathered implementation recommendations from experts and industry representatives, outlining key pressure points and exploring plausible ways to tackle them. The following paragraphs outline some of the critical recommendations voiced by stakeholders through the compendium.

Legitimate Interest

Similar to the European Union's (EU) General Data Protection Regulation (GDPR), consent is the bedrock on which India's DPDP Act stands: Personal data shall be processed only after obtaining consent from data principals. However, the consent-based approach does not consider the complex data-processing mechanisms of AI solutions, which involve other reasonable purposes to process. This could also cause a fall through the cracks as the determining legitimacy of consent is nebulous in AI operations. Therefore, it is essential to consider introducing 'legitimate interest' as one of the legal bases for processing data.

Publicly Available Data

The DPDP Act marks a pivotal juncture for AI technology essential for developing large foundational models and generative AI solutions. While the Act enables the utilisation of individuals' self-disclosed personal data, the emphasis on consent for processing publicly available information underscores a new era of accountability and debate over data access. It is essential to clarify the mechanism through which self-disclosed publicly available data is differentiated from other publicly available data.

Consultative Approach

It is imperative that the Ministry of Electronics and Information Technology (MeitY) undertakes extensive public consultations to finalise the DPDP Act Rules. These consultations should not be limited to the public but should also include special sessions with data fiduciaries dealing with different forms of data at sectoral levels to gain a comprehensive understanding of industry perspectives.

Transition Timeline

Provisioning a clear transition timeline is crucial, as organisations will need time to prepare, amend existing systems, and streamline processes to comply with the obligations mandated by the DPDP Act. Therefore, a phased timeline for implementing various compliance obligations is essential.

Privacy-enhancing Technologies

The DPDP Act Rules should emphasise the importance of utilising privacy-enhancing technologies, similar to those in other jurisdictions, to ensure seamless compliance with the Act.

Exemptions from the Act

To adopt a proportionate, risk-based approach, the government should consider exempting edtech providers from obtaining verifiable parental consent (VPC) under Section 9(1) of the DPDP Act and allow exceptions for behavioural tracking and monitoring under Section 9(3) when processing is solely for educational service provision. This exemption should be contingent upon the edtech providers

meeting specific standards and criteria to ensure adequate protection of children's data.

Lowering the Age Gate

Considering the widespread use of streaming platforms by Indian users for educational purposes, many of which offer free educational content, the Union government should evaluate the possibility of lowering the age for obtaining parental consent [in reference to Section 9(5)] for streaming platforms that provide child-friendly gateways for educational content in a 'verifiably safe' manner.

Alignment of Existing Regulatory Frameworks

Regulators such as the RBI, SEBI, and IRDAI must align their guidelines and policies with the DPDP Act's requirements. The Act should provide clearer guidelines to address potential overlaps between the legislation and existing sectoral regulations. Similarly, alignment is needed within regulations pertaining to the health sector.

Scenario-specific Guidelines

Clear guidelines are needed for specific data-processing scenarios, such as debt collection and fraud detection. Regulators must periodically review the DPDP Act's impact to ensure that it catalyses rather than impedes effective implementation across sectors.

Kamesh Shekar is Lead, Privacy and Data Governance vertical, and Co-lead, Artificial Intelligence vertical, The Dialogue.

ABOUT THE EDITORS

Kazim Rizvi is the Founding Director of The Dialogue, a public policy think-tank.

Shravishtha Ajaykumar is Associate Fellow at ORF's Centre for Security, Strategy and Technology.

ORF OBSERVER RESEARCH FOUNDATION
Ideas • Forums • Leadership • Impact

20 Rouse Avenue
New Delhi-110002
Ph: +91-11-43520020 Fax: +91-11-43520021
www.orfonline.org | info@orfonline.org

The Dialogue®
INFORM ENGAGE IDEATE

B-63, Lajpat Nagar - 1, New Delhi -110024
www.thedialogue.co | info@thedialogue.co