The Digital Personal Data Protection Act, 2023: Recommendations for Inclusion in the Digital India Act

Shravishtha Ajaykumar, Amoha Basrur
and Vaishnavi Sharma

Abstract

The new Digital Personal Data Protection Act (DPDPA) is market-friendly but is lacking in attention to privacy requirements for sensitive personal data. This report highlights three types of sensitive personal data—i.e., biometric, financial, and health—and emphasises the need for transparent consent mechanisms that will safeguard an individual's data. It underscores the role of data fiduciaries, urging the formulation of clear operational guidelines to enhance data protection and harmonising the relationships between data processors and fiduciaries to create a comprehensive regulatory system. The report outlines recommendations on the importance of adaptable data protection regulations and the need for governments to be accountable data fiduciaries to ensure that the upcoming Digital India Act is more inclusive and comprehensive.

Attribution: Shravishtha Ajaykumar, Amoha Basrur and Vaishnavi Sharma, *The Digital Personal Data Protection Act, 2023: Recommendations for Inclusion in the Digital India Act*, October 2023, Observer Research Foundation and The Dialogue.

Introduction

In August 2023, India announced its long-awaited Digital Personal Data Protection Act, 2023 (DPDPA).[1] The act expands on the rights of citizens beyond the Information Technology (IT) Rules, including the right to information, to correction and erasure, to grievance redressal, and to nominate a representative in the event of incapacity. It also outlines the requirements for Significant Data Fiduciaries (SDFs).[2] According to the Ministry of Electronics and Information Technology (MeitY), the DPDPA will soon be complemented by a Digital India Act (DIA) that will replace the existing IT Rules.[3]

In its present form, the DPDPA has gaps that need discussion. Among them is the absence of a provision guaranteeing a citizen's right to be forgotten[a] and the lack of explicit outlines and guidelines for sensitive personal data.[b]

On 27 September 2023, the Observer Research Foundation, in collaboration with the technology policy think-tank, The Dialogue, hosted a roundtable discussion on the DPDPA, specifically deliberating its impact on biometrics, financial, and health data. The roundtable gathered stakeholders from industry, civil society, and academia.

The participants agreed that while the DPDPA has ended the wait for a data privacy policy in India, it is only the first step for the country to successfully navigate the current era of emerging technologies.

The roundtable focused on three core areas, with the aim to inform the current gaps in legislation and contribute to future guidelines: Biometric data; Financial data; and Health data.

---

a The right to ask for one's data to be removed or deleted.

b This refers to biometric, financial, and health data, as defined in the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Biometric Data Panel

The proliferation of digital data has heightened concerns regarding data protection and privacy, necessitating the formulation of robust regulatory frameworks. This is especially true for data that is immutable from human and individual existence, such as biometric data. In the DPDPA, there are gaps in considerations for biometric data and its different forms, including in the definitions, purpose limitations, and responsibilities of data fiduciaries.

Explicit definitions

The DPDPA needs to establish well-defined terms in the DPDPA. These definitions should encompass sensitive data and consent as well as foundational data protection elements. The ambiguity in the current legislation creates scope for misuse, especially in the context of indirect data gathering and sharing of biometric data. An explicit definition of 'lawful purpose' also needs be defined, as mentioned in the IT Rules, 2011.[4] There is also a need to include definitions that extend beyond the current norm of biometric data collection to include second-generation or behavioural biometrics.[c,5] These definitions need to be cited alongside relevant purpose limitations.

c 'Behavioural biometrics' can refer to an individual's interactions with a digital interface or observable actions that are monitored and stored, including facial expressions and hormone mapping.

Implications of consent mechanisms

Consent is a cornerstone of data protection, and its efficacy hinges on the clarity and comprehensibility of consent processes. Including consent mechanisms and the 'right to be forgotten' is essential to saving and sharing data.[6] This is a primary concern, especially in areas where data can be shared with third parties for business purposes or through acquisition. Given the potential repercussions of an individual's ability, or lack of it, to make informed decisions about their data, there is a need for standardised and easily understandable consent mechanisms.

Data fiduciaries and trust mechanisms

Data fiduciaries are entrusted with safeguarding personal data, making them central figures in protecting an individual's privacy. However, the practicality and effectiveness of data fiduciaries hinge on clear operational instructions and the standardisation of consent processes. The law must therefore provide data fiduciaries with clear guidelines and best practices to enhance data protection.

The roundtable highlighted three critical Ts:

1. Trust among stakeholders;

2. Transparency in the context of establishing a transparent, clear, and understandable policy ecosystem;

3. Techno-regulatory frameworks, which require active efforts towards creating a harmonious understanding and implementation of law and technology.

Financial Data Panel

A primary concern around financial data is determining the proper authority and relevant data standards. Fintech regulators must proactively underline data and privacy protection specifics, especially owing to the broad range of the DPDPA. Here, sectoral intersections are encouraged and inevitable when regulating personal financial data, and coordination and harmonisation between sectors is essential to developing a comprehensive framework.

Industrial implementation experiences

The current version of the DPDPA is largely industry-friendly, as it does not require significant additional changes from fintech firms that were not already delineated by authorities like the Reserve Bank of India. These rules familiarise fintech agencies with essential lexicon related to areas such as consent, consent managers, and purpose limitation.[7,8]

Relationship between data processors and fiduciaries

With the DPDPA, the relationship between data processors and fiduciaries in the fintech space has become more level and precise, with both the data fiduciaries and data processors mandated to maintain and adhere to data and privacy protection standards. This is also true in the fintech space and needs to be extended to the banking sector through establishing a comprehensive relationship between data processors and SDFs.

Considering emerging technologies

Various provisions of the DPDPA, such as Section 3(c)(ii) read with Section 7, regulate emerging technologies. However, the Act does not directly provide for the regulation of emerging technologies.[9] The panel discussion highlighted how emerging technologies such as artificial intelligence (AI) can be leveraged to provide personalised services, better service delivery, and transparent data processing, as well as aid processors to effectively protect financial data. It was also noted that there is a need for enhanced encryption techniques and the introduction of better user consent mechanisms that move beyond consent as a threshold.

Health Data Panel

The absence of a sectoral bill for healthcare was a significant concern that was raised during the discussion. The DPDPA does not define or classify health data—a failing that participants flagged as a prerequisite for effective data management especially as the DPDPA does not define 'harm' and focuses on 'breaches' instead. Specific and comprehensive legislation for health data management is required to go beyond merely addressing data breaches in order to protect individuals from the various forms of harm that can result from the misuse of health data.[10,11] To fill this gap, a version of the Digital Information Security in Healthcare Act, 2018 (DISHA) could be reintroduced.

Additionally, existing regulations must adequately cover the rapid proliferation of emerging technologies such as wearable devices. Bringing this data under rule through a uniform framework will drive research in the sector, instil consumer confidence, and reduce regulatory complexities.[12]

Defragmenting the policy ecosystem

Amidst a slew of proposed health legislations and initiatives such as the Health Management Policy and Unified Health Interface, the fragmentation of policies related to healthcare data was another primary concern that was highlighted during the roundtable. Healthcare data legislation and procedures must be consolidated into a comprehensive framework. Referencing countries with well-established healthcare and data policies could provide insights into bridging gaps in existing regulations.[13]

Prioritising skilling for cybersecurity

Recent incidents of health systems insecurity and cybercrime are opportunities for technological and governmental improvements in data protection. Providing training and skill development for cybersecurity professionals is essential to overall data security efforts.[14]

Data sharing and privacy

Data sharing is a field that is difficult to regulate and is made more complicated with exclusions for minors and checkpoints. The data of minors needs to be addressed in isolation of permissions granted by their guardians. Additionally, there is a need for gradations in age groups and authority over data, including the statute of limitations for permissions granted by guardians.

Checkpoints and guidelines for security frameworks and measures are urgently required to ensure health data privacy, anonymisation, and purpose limitations. Sector-specific international standards such as the Standards for Privacy of Individually Identifiable Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and ISO 27799 can also provide frameworks to develop domestic guidelines.[15,16]

The Unified Payments Interface architecture can offer an example of preventing the gatekeeping of data and maximising consumer choice. This approach reduces the ability to monetise customer acquisition. The discussion further highlighted the advantages of increased interoperability in the healthcare ecosystem, including enhanced efficiency from seamless health data exchange, which can improve care coordination and patient outcomes; reduced duplication of effort and costs; more accurate and comprehensive health data analysis; and the development of new technologies to improve healthcare delivery and patient engagement.[17]

Recommendations

A critical aspect under scrutiny was holding governments accountable as data fiduciaries. Additionally, the discussion emphasised the importance of clearly defining the exemptions for storing data for 'lawful purposes'.

The ORF-The Dialogue roundtable shed light on a number of critical aspects that require careful consideration and further action in the context of the forthcoming DIA. The importance of data protection and privacy in an era of unprecedented data generation and exchange cannot be overstated, and these regulations need to be comprehensive and practical, and adaptable to the evolving technological landscape.

The roundtable underscored the need for well-defined terms and consent mechanisms in the context of biometric data. Precise definitions of concepts such as 'sensitive data', 'consent', and 'lawful purposes' are essential to prevent misuse and ensure that individuals can make informed decisions about their data. Data fiduciaries, who play a pivotal role in data protection, must have clear operational guidelines to fulfil their responsibilities effectively.

The DPDPA is already industry-friendly for financial data and aligns with existing regulatory standards. However, harmonising data processors and fiduciaries ensures a level playing field across different sectors. The regulation of emerging technologies such as AI should be addressed explicitly to harness their potential for enhancing data protection.

In the context of health data, the absence of a sectoral bill for healthcare is a significant concern. A dedicated legislation for health data management is required to go beyond addressing breaches and protecting individuals from potential harm. Consolidating healthcare data legislation and procedures into a comprehensive framework is vital to prevent fragmentation. Cybersecurity and risk-based approaches in healthcare data protection cannot be understated.

Across all areas, there were commonalities in the recommendations regarding additions to the data regulation regime outside of vertical regulation. These recommendations include:

a. Establishing definitions that include and truncate additions in sensitive personal data;

b. Including growing and emerging technologies in regulations;

c. Creating comprehensive policy ecosystems and curtailing fragmentation.

As India moves towards implementing the DIA to complement the DPDPA, it is essential to incorporate these recommendations and ensure that the regulatory framework is robust and adaptable to the ever-changing digital landscape. Additionally, holding governments accountable as significant data fiduciaries and defining exemptions for data storage for lawful purposes are crucial steps in ensuring the effectiveness of data protection and privacy regulation in India.

Annex

Immutable Data: The Future of Privacy in the Context of Biometrics, Financial Data and Health Data
27 September 2023
Delhi

Attendees

Moderators

Shravishtha Ajaykumar, Observer Research Foundation

Amoha Basrur, Observer Research Foundation

Kazim Rizvi, The Dialogue

Kamesh Shekar, The Dialogue

Speakers

Angelina Dash, Centre for Communication Governance, National Law University Delhi

Pushan Dwivedi, CRED

Himanshi Gautam, RELX

Saranya Gopinath, Razorpay

Indranath Gupta, Jindal Global Law University

Nikhil Iyer, The Quantum Hub

Tejaswita Kharel, Centre for Communication Governance, National Law University Delhi

Binoj Koshy, Unique Identification Authority of India

Rakesh Maheshwari, Ex-Ministry of Electronics & IT

Shweta Mohandas, Centre for Internet Security

Reshu Natani, Amazon Web Services

Lalit Panda, Vidhi Centre for Legal Policy

Jayadev Parida, School of Liberal Studies, University of Petroleum and Energy Studies

Radhika Roy, Internet Freedom Foundation

Jameela Sahiba, The Dialogue

Krishna Ravi Srinivas, Research and Innovation Systems for Developing Countries

Cover photo: Getty Images/imaginima

Endnotes

1 Ministry of Electronics and Information Technology, Government of India, "The Digital Personal Data Protection Bill, 2023," *Ministry of Electronics and Information Technology*, www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

2 Ministry of Electronics and Information Technology, Government of India, "The Digital Personal Data Protection Bill, 2023."

3 Ministry of Electronics and Information Technology, Government of India,, "Digital India Act," *Press Information Bureau*, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1948357.

4 "IT Rules Sensitive Personal Data or Information (SPDI) Rules." *Sensitive Personal Data or Information (SPDI) Rules*. https://indiankanoon.org/doc/114407484/.

5 Shravishtha Ajaykumar, "Ethical and Regulatory Considerations in the Collection and Use of Biometric Data," *Observer Research Foundation*, October 10, 2023, https://www.orfonline.org/research/ethical-and-regulatory-considerations-in-the-collection/.

6 "Right to Be Forgotten - The Digital Personal Data Protection Bill, 2023." *PRS Legislative Research*, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023.

7 Ministry of Finance, Government of India, "Account Aggregator Network- a Financial Data-Sharing System." *Press Information Bureau*. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1753713.

8 Reserve Bank of India, "Account Aggregator (Reserve Bank) Directions," *Reserve Bank of India,* https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598.

9 Kamesh Shekar, "Analysis Comparative Analysis of India's Digital Personal Data Protection Bill 2022, and 2023" *The Dialogue*, August 4, 2023. https://thedialogue.co/wp-content/uploads/2023/08/Designed-finalDPDPB-2023_Analysis-Paper.pdf.

10 Stefan Germann et al., "Realising the Benefits of Data-Driven Digitalisation without Ignoring the Risks: Health Data Governance for Health and Human Rights," *mHealth*, October 2020, https://doi.org/10.21037/mhealth-2019-di-11.

11 Adil Hussain Seh et al., "Healthcare Data Breaches: Insights and Implications," *Healthcare*, May 13, 2020, https://doi.org/10.3390/healthcare8020133.

12 Avirup Dasgupta et al., "A Conceptual Framework for Data Governance in IoT-Enabled Digital IS Ecosystems," *Proceedings of the 8th International Conference on Data Science, Technology and Applications* (2019), https://doi.org/10.5220/0007924302090216.

13 Shweta Mohandas, "Health Data Management Policies - Differences Between the EU and India," *The Centre for Internet and Society* (2023), https://cis-india.org/internet-governance/blog/health-data-management-policies.

14 "Bridging the Gap- Identifying Challenges in Cybersecurity Skilling and Bridging the Divide," *Data Security Council of India* (2023), https://www.dsci.in/files/content/knowledge-centre/2023/Bridging-the-Gap-Identifying-Challenges-in-Cybersecurity-Skilling-and-Bridging-the-Divide.pdf

15 United States Department of Health and Human Services, Federal Government of the United States of America, "Summary of the HIPAA Privacy Rule," *United States Department of Health and Human Services*, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

16 "Health informatics — Information security management in health using ISO/IEC 27002 (ISO 27799:2016)," *International Standards Organization* (2016), https://www.iso.org/standard/62777.html.

17 "Health Data Governance: Privacy, Monitoring and Research - Policy Brief," *Organization for Economic Cooperation and Development* (2015), https://www.oecd.org/health/health-systems/Health-Data-Governance-Policy-Brief.pdf.

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org