इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY

सत्यमेव जयते

मानकः पथप्रदर्शकः
Bureau of Indian Standards

Workshop on Practical Aspects of Digital Personal Data Protection Act, 2023 Implementation

Policy Brief

Ashank Desai
Centre *for* Policy Studies
Indian Institute of Technology Bombay
Insight ♦ Dialogue ♦ Impact

IITB TRUST LAB
DIGITAL : SECURE : RESPONSIBLE

November 2024

Executive Summary

This policy brief summarises the key insights from a workshop organized by the Ashank Desai Centre for Policy Studies and TrustLab at IIT Bombay, in collaboration with the Ministry of Electronics and IT (MeitY) and the Bureau of Indian Standards (BIS), on November 30, 2024, to address implementation challenges of the Digital Personal Data Protection (DPDP) Act 2023. The workshop brought together stakeholders from government, industry, and academia.

The workshop focused on four critical areas: overview of the Act, role of standards, consent management, and data protection. Through structured breakout sessions, participants identified key implementation challenges and proposed practical solutions. The workshop emphasised the importance of continued stakeholder engagement in addressing implementation challenges.

Advisory Committee for the Workshop

Prof. Sundeep Oberoi (Chair) – ADCPS IIT Bombay

Prof. S. Sudarshan – Dept of CS&E IIT Bombay

Prof. S.K. Jha – ADCPS IIT Bombay

Prof. R.M. Sonar – SJMSOM IIT Bombay

Mr P.P. Singh – Group Chief Information Security & Privacy Officer, Avenue Supermarts Ltd

Workshop on Practical Aspects of DPDP Act 2023 Implementation
Policy Brief

1. Introduction

India now has a personal data protection law, the Digital Personal Data Protection (DPDP) Act 2023[1]. With the legislative process completed, the attention has shifted to the Act's implementation. The spotlight now turns to various stakeholders, who must take the necessary steps to meet the obligations of the legislation. However, several procedural and practical challenges remain to be identified and addressed to ensure an effective implementation of its provisions.

Ashank Desai Centre for Policy Studies and TrustLab at IIT Bombay[2] organised a participative workshop in collaboration with the Ministry of Electronics and Information Technology (MeitY) and the Bureau of Indian Standards (BIS) to elicit stakeholder views on possible challenges and solutions. Stakeholders from the government, industry, and academia joined in deliberating on four critical topics: an overview of the Act (legal, technical and organisational aspects), the role of standards, consent management, and data protection. The stakeholder participation is shown in Figures 1 and 2, showcasing the distribution of participants across different roles and their organisational affiliations, demonstrating diverse engagement.

[1] DPDP Act 2023
[2] Ashank Desai Centre for Policy Studies and TrustLab

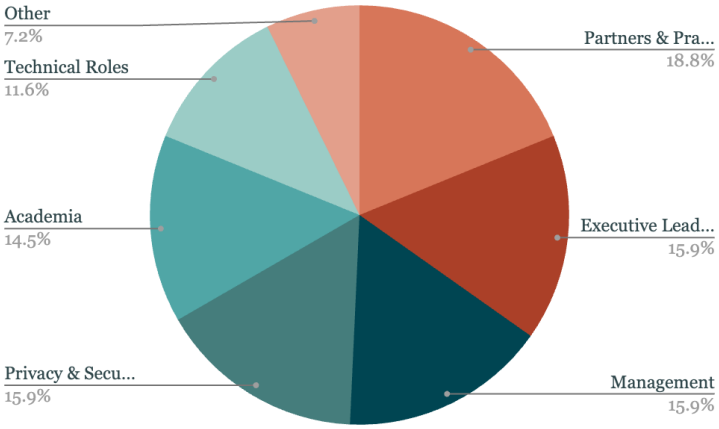

Figure 1: Role distribution

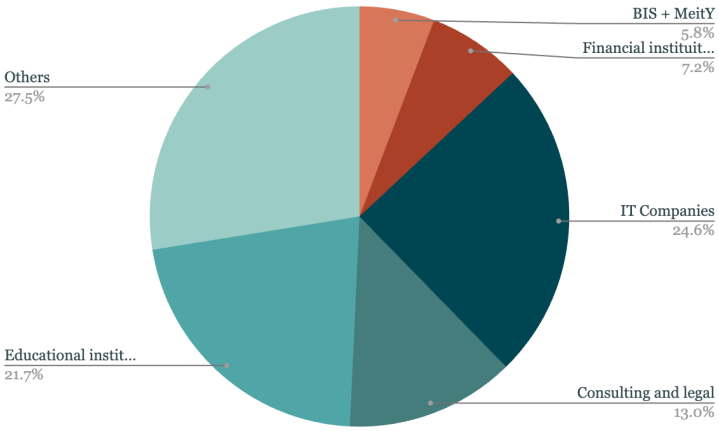

Figure 2: Organization Distribution

Building on this multisector representation, this brief highlights the key insights and recommendations that emerged from the workshop.

2. Workshop Structure and Session Overviews

The workshop was structured into four sessions, each introduced by a subject matter expert and followed by breakout discussions. Participants were asked to address specific questions related to each topic. Questions for each session were formulated by the key stakeholders and the advisory committee, as presented in Table 1.

Topic Name	**Brief Introduction**	**Questions Given to Discuss in Breakout**
Overview of the Act	Representatives from MeitY presented an overview of the DPDPA 2023, highlighting the Act's key provisions. Privacy-enhancing techniques were introduced, such as data masking, encryption, and data anonymisation.	1. What procedure will the Data Protection Board follow? Will it be the Code of Civil Procedure or something else? 2. How will alleged violations of the provisions of the Act be investigated? 3. What are the practical impediments to a completely digital office for the Data Protection Board? 4. What kind of technological intervention can help entities comply with the DPDP Act?
Role of Standards	Representatives from BIS presented existing standards on IT Security and Privacy. They also highlighted the need for standards mentioned in the DPDP Act.	1. Are the current standards available sufficient to implement the provisions of the Act efficiently? 2. If the current standards are not sufficient, what are the specific 3-4 items that need to be standardised?

Topic Name	Brief Introduction	Questions Given to Discuss in Breakout
		3. How can this standardisation gap (if it exists) be addressed in the next 6-12 months?
Consent Management	Mr Sachin Khalap presented the Session. Discussed in the context of the DPDP Act, focusing on scenarios for consent collection, business models for consent managers, and creating standard formats for consent.	1. In what scenarios must consent be collected? 2. What is the business model for a consent manager? 3. How do we create a standard format for "Consent" and the underlying "Purposes"? 4. What role can Account Aggregators play with respect to Consent management?
Data Privacy and Protection	The session presented by Mr PP Singh focused on differentiating data breaches, determining reasonable data protection, identifying data leak sources, and assessing traditional techniques like encryption.	1. Differentiate between data breach and personal data breach. 2. Determine what is reasonable data protection. 3. Identify the source of a data leak, given similar data points held across multiple providers. 4. Ascertain if traditional data protection techniques like encryption are sufficient in the context of Privacy.

Table 1: Topics and Questions

3. Discussions and Key Insights

The workshop included breakout discussions across all four sessions, with participants identifying key implementation challenges and proposing practical solutions. Table 2 summarises the main discussions, challenges identified, and key takeaways from each session.

Session Topic	Key Discussions	Challenges Identified	Key Takeaways
Overview of the Act	• A brief discussion around the aim of the Act: to protect personal data while enabling its processing. • Implementation of SARAL: Simple, Accessible, Rational, and Actionable. • The priority of the law is 'individual consent' for the use of personal data. • The Act prioritises ease of doing business. • Data may be processed without consent only in legitimate cases where the state or its agencies perform	1. Functioning and execution of the Digital Protection Board. 2. DPB is not a regulatory body; who or what will be the final signing authority? 3. Ambiguity around the investigation procedure in case of violations of the Act. 4. Challenges with respect to a completely 'digital' board: no walk-in complaints, digital access, awareness of the law, etc. 5. Questions around demonstrating compliance.	1. Largely the Code of Civil Procedure will be used by the Board who may evolve and use some other procedure for the more technical aspects of its work. 2. The Board does have the power to request the services of any police officer or any officer of the central or state government and such officers are required to comply. with such requests. 3. It is not clear what the volume of complaints is likely to be and so whether all complaints will directly go to the board or there will be some method to investigate the veracity of a complaint before it is taken up by the Board.

Session Topic	Key Discussions	Challenges Identified	Key Takeaways
	functions under the law.		
Role of Standards	• Highlight on current standards landscape: ISO 27001, ISO 17428, IS 29184.	1. Unawareness of available standards. Lack of implementation-level standards. 2. Lack of technical standards as compared to management standards. 3. There is a need for sector-specific standards rather than a one-size-fits-all approach.	1. Current standards need comprehensive review in light of DPDPA 2023 2. Sector-specific approach more practical than universal standards. 3. Implementation-level guidelines needed alongside management frameworks. 4. Need for clearer audit mechanisms. 5. Balance needed between prescriptive standards and flexible guidelines.
Consent Management	• A brief discussion on Consent with respect to the DPDPA. • A comparison of the DPDPA with the GDPR shows that there is no reference point for a global consent manager. • New-age digital businesses need a seamless consent	1. Lack of clarity on the workflow between Data Principals, Consent Managers and Data Fiduciaries 2. Lack of clarity on the role and responsibilities of the consent manager. 3. Uncertainty about whether consent manager should be internal or third-party 4. Lack of clarity on standard	1. Since the workflow of consent management, especially dataflow between Data Principals, Consent Managers and Data Fiduciaries is not clear, it is difficult to assess the impact and changes to existing systems 2. It was felt that Data Principals were unlikely to agree to accept to pay consent managers. In light of this Data Fiduciaries could get into contractual agreements with Consent Managers to handle

Session Topic	Key Discussions	Challenges Identified	Key Takeaways
	framework and unique approaches required for different types of businesses. • Consent must serve legitimate purposes and avoid unnecessary data collection. • Consent managers should act as data providers and aggregators and function as data custodians.	format for consent across sectors. Issue of digital literacy gaps in India and navigating India's socio-economic diversity.	consent management free for their own users. If a Data Principal wants to use another consent manager then that Data Principal would have to bear the charges for the chosen manager
Data Privacy and Protection	• The DPDPA mandates Data Fiduciaries and Processors to protect personal digital data through security safeguards, defining a breach as any unauthorized or accidental compromise of data's confidentiality, integrity, or availability.	1. Lack of clarity between personal vs non-personal data. 2. There is no clear definition of "reasonable compliance" 3. Difficulty in recognising and establishing data breaches. 4. Accountability issues include non-liability of data processors under the DPDPA, data	1. Industry-level, sector wise and organization level policies, regulations, and compliance measures are required for data protection. 2. Need for an operational definition of what constitutes "reasonable" compliance. 3. Implementation of Privacy Enhancing Technologies (PET). 4. Need for innovating the concept of "know-your-data". 5. Creation of empanelled

Session Topic	Key Discussions	Challenges Identified	Key Takeaways
	• Discussion on key control areas in the domain of protection and privacy: operational (rules and processes), administrative (policies), architectural (system connections), technical (security controls), response (incident handling), and visibility (threat detection)	brokers bypassing the law, and lack of contract-based accountability. 5. Implementation challenges such as balancing security with operational efficiency, consent is often hidden or partial rather than informed.	auditors with clear guidelines. Data volume and data usage are important factors in the classification of data into personal and non-personal data - DPDPA rules must consider both the factors.

Table 2: Discussions and Insights from the Workshop

4. Conclusion

The workshop highlighted several critical aspects of implementing the Digital Personal Data Protection (DPDP) Act 2023. Through structured sessions covering four key areas – overview of the Act, role of standards, consent management, and data privacy and protection – participants identified challenges and gave recommendations for implementation.

A key theme across sessions was the need for clarity in operational definitions and procedures. This includes establishing clear workflows between Data Principals, Consent Managers and Data Fiduciaries, determining reasonable data protection measures, and developing sector-specific approaches rather than a one-size-fits-all standard.

As the attention shifts to the Act's implementation, continued stakeholder engagement and review of implementation challenges remains crucial. The insights from this workshop can help relevant stakeholders in formulating the DPDP rules and ensuring adequate protection of personal digital data.

5. Post- Script

Since the workshop discussed in this brief, there has been a significant development in the journey of the DPDP Act. On January 5th, 2025, MeitY published the draft rules for DPDPA, opening them for stakeholder feedback until February 18th.

MeitY has been proactively engaging with stakeholders through consultation meetings across major cities, including Delhi and Mumbai. These consultations have brought together diverse participants from technical, legal, banking, insurance, and financial sectors, representing both government and private entities.

The Mumbai consultation revealed that stakeholders did not seek significant changes to the Act or rules. The main focus was on clarifying legal language and simplifying complex terms. For instance:

- Rule 15, which provides an exemption from the Act for research, archiving, or statistical purposes, raised concerns about the broad meaning of "statistical purposes." Stakeholders asked for a clearer definition and scope.
- Rule 12(3), which requires Significant Data Fiduciaries to verify algorithmic software, was questioned for being too broad. The term "algorithmic software" could mean any type of algorithm requiring more specific guidelines.

A key insight from both the workshop and consultations is that implementing the DPDPA's provisions will require major changes to existing IT infrastructure and systems. Going forward, MeitY should initiate focused consultations with **technical implementation experts**. With an implementation window of 12-24 months, there is an urgent need to begin the technical planning and formulate technical standards.

As the implementation phase progresses, continued engagement between policymakers, technical experts, and industry stakeholders will be essential for the Act's successful implementation.