Digital Personal Data Protection Act & Rules: Key Insights from Mehta & Mehta Webinar

The Digital Personal Data Protection Act, 2023 (DPDP Act) marks a transformative shift in India's legal and regulatory framework governing personal data. In a recent knowledge-sharing webinar organised by Mehta & Mehta, experts from the legal, compliance, and technology domains examined the background, scope, key concepts, and practical compliance implications of the Act.

The session witnessed active participation from company secretaries, chartered accountants, legal professionals, compliance officers, and industry representatives, reflecting the widespread impact of the DPDP Act across sectors and organisational sizes.

Background and Need for the DPDP Act

The DPDP Act is rooted in the landmark judgment of the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) v. Union of India, which recognised the right to privacy as a fundamental right under Article 21 of the Constitution. While this constitutional recognition established privacy as a core civil liberty, it did not, by itself, create an enforceable operational framework.

As discussed during the webinar, the absence of a comprehensive data protection law resulted in fragmented regulation under the Information Technology Act, 2000 and sector-specific guidelines issued by regulators such as RBI and IRDAI. These frameworks lacked uniform standards on consent, data minimisation, accountability, and breach reporting.

Rapid digitalisation of India's economy, proliferation of mobile applications, digital payments, e-commerce, Aadhaar-linked services, and data-driven business models led to exponential growth in personal data processing. This, coupled with increasing instances of data breaches, misuse of personal information, and opaque consent mechanisms, necessitated a robust, technology-neutral, and enforceable data protection regime.

The DPDP Act also aligns India with global privacy frameworks such as the EU General Data Protection Regulation (GDPR), thereby facilitating cross-border data flows, strengthening investor confidence, and enhancing trust in India's digital ecosystem.

Applicability and Territorial Scope

The DPDP Act applies to:

Digital personal data collected within India; and • Personal data collected outside India, if such processing is in connection with offering goods or services to data principals within India.

The Act covers personal data collected in digital form as well as data initially collected in non-digital form but subsequently digitised. Certain exclusions apply, including processing for personal or domestic purposes, publicly available data, and specific exemptions for State functions such as national security, public order, research, and statistical purposes.

Phased Implementation Timeline

The webinar highlighted that the DPDP Act is being implemented in a phased manner:

Foundational provisions, definitions, and establishment of the Data Protection Board became effective from 13 November 2025; Provisions relating to Consent Managers are expected to become enforceable from November 2026; and Full enforcement of the Act and Rules is scheduled for 13 May 2027.

This staggered implementation provides organisations with a limited transition window to design, implement, and test their data governance frameworks.

Key Concepts under the DPDP Act

Personal Data

Personal data is defined as any data about an individual who is identifiable by or in relation to such data. Identification may be direct (such as name, mobile number, Aadhaar, PAN) or indirect, where multiple data points collectively identify an individual (such as device identifiers, IP addresses, or behavioural data).

Notably, the DPDP Act does not categorise data into sensitive or non-sensitive classes. All personal data is uniformly protected, shifting the compliance focus to purpose limitation, consent, and accountability.

Processing

Processing is defined broadly and includes any operation performed on digital personal data, such as collection, storage, use, sharing, disclosure, analysis, profiling, or erasure. The panel emphasised that even passive storage or retention of personal data constitutes processing and triggers compliance obligations.

Data Principal

A data principal is the individual to whom the personal data relates. In the case of children or persons with disabilities, parents or lawful guardians act on their behalf. Customers, employees, patients, users of digital platforms, and beneficiaries of services are all data principals under the Act.

Data Fiduciary

A data fiduciary is any person or entity that determines the purpose and means of processing personal data. This includes companies, LLPs, partnerships, government departments, NGOs, professional firms, and employers.

Examples discussed during the webinar included banks processing KYC data, employers managing employee records, hospitals maintaining patient information, and digital platforms profiling users for service delivery or advertising.

Significant Data Fiduciary

Certain data fiduciaries may be classified as Significant Data Fiduciaries based on factors such as volume and sensitivity of data processed, risk of harm to data principals, and use of emerging technologies such as artificial intelligence.

Such entities will be subject to enhanced compliance obligations, including:

Appointment of a Data Protection Officer; Conduct of Data Protection Impact Assessments; Independent audits; and Greater regulatory oversight.

Sectors such as banking, insurance, healthcare, fintech, and large digital platforms are expected to fall within this category.

Data Processor

A data processor processes personal data strictly on behalf of a data fiduciary and does not determine the purpose of processing. Cloud service providers, payroll processors, KYC vendors, payment gateways, and HR software providers typically act as data processors.

The webinar underscored the need for revisiting vendor contracts to clearly define fiduciary–processor roles, impose data protection obligations, mandate breach notifications, and ensure minimum cybersecurity standards.

Consent and Consent Managers

Consent lies at the heart of the DPDP Act. Consent must be free, specific, informed, unconditional, unambiguous, and provided through clear and plain language.

A unique feature of the Indian framework is the concept of Consent Managers. Consent Managers are independent entities registered with the Data Protection Board that enable data principals to give, manage, review, and withdraw consent through an interoperable platform.

The panel noted that this system aims to address consent fatigue, opaque fine-print agreements, and lack of meaningful choice by empowering individuals with greater control and transparency over how their data is used.

Practical Compliance Challenges and Insights

Speakers emphasised that DPDP compliance is not merely a legal exercise but a significant operational and cultural shift. Organisations must undertake:

Data mapping and inventory to identify what data is held, where, and for what purpose; Data minimisation and deletion of legacy data without lawful purpose; Revision of privacy notices, consent forms, and internal policies; Employee training and awareness to embed privacy into organisational culture; and Strengthening cybersecurity controls and incident response mechanisms.

Special attention was drawn to risks arising from excessive data collection by mobile applications, intrusive tracking technologies, and use of personal data beyond stated business purposes.

Conclusion

The Digital Personal Data Protection Act, 2023 represents a paradigm shift in how organisations in India collect, use, and safeguard personal data. While the law introduces significant compliance responsibilities, it also provides an opportunity to build trust, transparency, and resilience in the digital economy.

Organisations that proactively align their governance structures, contracts, and operational practices with the DPDP Act will be better positioned to manage regulatory risk and enhance stakeholder confidence.

To stay informed or access the webinar recording, visit the YouTube channel: 🎥 **"Decoding Corporate Laws with Mehta & Mehta"**