IBM India/South Asia Blog

Analyst Blog: Navigating India’s DPDPA - Data at the Heart of Secure Businesses

Apr 25, 2024

By Christian Fam, Research Manager, IDC

After years of deliberations and negotiations, India's Digital Personal Data Protection Act (DPDPA) was finally passed on August 11, 2023. The Bill underwent rapid progression, clearing both the lower and upper Houses of Parliament within just over a week. The DPDPA, modeled after the European Union's (EU) General Data Protection Regulation (GDPR), aims to establish a comprehensive framework for the protection of digital personal data, extending coverage to all entities that process personal data within India, regardless of size and private status.

It mandates robust security measures to prevent data breaches, with an obligation to notify both the Data Protection Board of India and affected individuals in case of a breach, highlighting a strong stance on data protection and accountability.

In a nutshell, the DPDPA emphasizes the importance of data privacy, protection, consent, transparency, and accountability in data processing activities. This blog will lay out some of the most important aspects of the DPDPA and explore the implications of how organizations processing digital personal data within India should respond and prepare for such changes.

Compliance Takes Center Stage

With such drastic changes already in motion, Indian enterprises are undoubtedly on edge, struggling to abide by the new Act whilst balancing growth and innovation. According to IDC’s AP IT and Business Services Sourcing Survey, 2023, businesses in India have highlighted that ensuring a lawful basis for data processing (43.4%) ranks as their top concern regarding compliance with data privacy regulations. This is followed by data anonymization (41%), data sovereignty/cross-border transfer restrictions (39.8%), and security and privacy integration (37.3%). This underscores the paramount importance placed by Indian organizations on adhering to lawful mandates for data processing to mitigate risks, safeguarding individual privacy rights, and upholding regulatory compliance standards.

Additionally, in recent studies conducted by IDC, it has become evident that Indian enterprises are increasingly emphasizing the importance of safeguarding their data and intellectual property from security threats. This heightened focus on security

measures is not merely about fortifying their cyber defenses; rather, it extends to a broader objective of enhancing digital trust within the organization and with external stakeholders.

The enactment of the DPDPA presents a complex compliance landscape for Indian enterprises. Organizations are now tasked with navigating stringent consent requirements, ensuring data integrity, and implementing robust protection measures. The challenges are multifaceted, ranging from technological upgrades to procedural overhauls, all aimed at safeguarding personal data against breaches and misuse. Failure for non-compliance will result in hefty penalties, underscoring the act's emphasis on accountability:

- **Minor breaches:** Fines can range up to INR 250 Crores (approx. US$30 million) or 2% of the entity's global turnover, whichever is higher. These minor breaches encompass failures in reporting breaches or non-compliance with data processing standards.
- **Major breaches:** For more severe violations, such as unauthorized sharing or processing of personal data without consent, penalties can escalate to INR 500 Crores (approx. US$60 million) or 4% of the annual global turnover.

Robust Data Governance: A Necessity

In the wake of the DPDPA's implementation, robust data governance emerges not just as a compliance requirement but as a strategic imperative. Data governance encompasses the policies, standards, and practices that ensure the effective and efficient management of data assets. It serves as the backbone for achieving compliance, enhancing data security, and fostering trust among stakeholders.

Without an overarching data governance strategy, Indian organizations may find themselves unable to comply with the DPDPA or guarantee data privacy and protection. Rather than hastily attempting to adhere to the DPDPA, it's crucial to meticulously outline data protection strategies, policies, and procedures. This approach should include classifying data based on sensitivity, defining its usage, identifying and cataloging critical data assets, and implementing operational resilience strategies such as data backup plans. Only once data governance has been established can Indian organizations look towards technological security solutions to carry out their plan for robust data security, privacy, and compliance.

Leveraging Security Solutions for Compliance and Trust

As organizations operating in India navigate the complexities of data protection and compliance, leveraging robust security solutions becomes essential. Such solutions should not only address the entire end-to-end data lifecycle but must offer a comprehensive suite of capabilities designed to safeguard sensitive data, enforce compliance policies, and mitigate risks associated with data breaches. For example, IBM's data security offerings are built around a holistic approach to data protection, designed to provide comprehensive visibility, real-time monitoring, and automated compliance reporting across diverse data environments.

In today's vast security market, organizations in India seeking data protection and compliance solutions should prioritize offerings with the following key features:

- **Real-time data discovery and classification:** Automates the identification and classification of sensitive data across various environments, facilitating compliance with the DPDPA.
- **Data protection through encryption and masking:** Enhances data security at rest and in transit, crucial for preventing data breaches and complying with DPDPA's encryption mandates.
- **Data activity monitoring:** Enables real-time tracking of data access and activities, ensuring adherence to DPDPA's access control and data handling policies.

- **Continuous compliance monitoring:** Assists in maintaining and demonstrating regulatory compliance, allowing organizations to identify and rectify security and compliance issues promptly.

According to IDC's AP IT and Business Services Sourcing Survey, 2023, in the next two years, data protection, governance, and compliance solutions (39.8%) will be the second largest investment area for Indian enterprises, after attack surface management (41%). This highlights that, despite the operational complexities and costs associated with meeting new regulatory mandates, organizations in India are emphasizing data protection and compliance. Their goal is to foster trust with customers, vendors, and partners, recognizing the strategic value of robust data governance in today's digital landscape.

Conclusion

Although it is important to note that the law will not come into effect until the government provides notice of an effective date, Indian and global businesses alike must be prepared for the regulatory mandates that are bound to shape how businesses operate. To thrive in India's data-driven economy, forward-thinking businesses will be sure to explore and adopt robust data security solutions, offered by technology giants such as IBM, not only as a regulatory imperative but also as a strategic necessity. By prioritizing data protection and compliance, businesses operating in India can uphold consumer trust, mitigate legal and reputational risks, and drive sustainable growth in this fast-expanding digital-first era.

Christian Fam, Research Manager, IDC

The views and opinions expressed above are exclusively of the author(s) and not of any other individual or institution. The data and figures mentioned above are based on IDC's analysis of the Indian market.

Blog Categories