September 2024

DUA ASSOCIATES

IN BRIEF

NAVIGATING THE NEW ERA OF DATA PROTECTION FOR BUSINESSES

I. The New Data Protection Landscape

The Digital Personal Data Protection Act, 2023 (DPDPA) received the assent of the Hon'ble President of India on August 11, 2023. While the DPDPA has not yet been enforced, its implementation is expected soon, which will mark a pivotal moment in India's regulatory framework for data protection.

As businesses expand both within India and globally, the DPDPA holds significant importance, especially given the rapid rise of artificial intelligence (AI) and the growing value of data in today's digital economy. Currently, businesses and body corporates in India must comply with Section 43A of the Information Technology Act, 2000 (IT Act). This provision, introduced through the Information Technology (Amendment) Act, 2008, imposes liability on organizations that possess, handle, or deal with sensitive personal data. If a company fails to implement or maintain reasonable security practices and procedures, and this negligence results in unauthorized access, use, or disclosure of personal data, they can be held liable for compensating the affected individuals for the resulting damages.

The definition of "reasonable security practices" is provided under Explanation (ii) to Section 43A of the IT Act, which refers to security measures designed to protect personal data from unauthorized access, use, modification, or impairment. These practices can either be defined through mutual agreements between parties or prescribed by the government in consultation with relevant professional bodies.

With the enactment of the DPDPA, however, Section 43A of the IT Act will be omitted, signaling a shift from the IT Act's framework to a more comprehensive and modern data protection regime under the DPDPA. This transition will also lead to the repeal of the 2011 "Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules", which were enacted under Section 43A of the IT Act.

Expected to be framed soon, the rules under the DPDPA will provide clarity on compliance requirements for businesses, which will define operational details, such as how businesses should handle personal data, reporting of breaches, consent mechanisms, and penalties for non-compliance. The rules are expected to align with global data protection standards and address new challenges posed by emerging technologies like AI, ensuring that India's legal framework remains robust and adaptable to the evolving digital landscape.

II. Building a Strong Data Protection Framework - A Step-by-Step Guide

Under the DPDPA, businesses must establish a robust data security and privacy system. This involves the following key steps:

(i) Assessment - Start by reviewing and identifying areas that need improvement within your current data protection and privacy framework. Develop a structure that addresses potential risks, which may require capital investment to upgrade technological solutions, mitigate risks, and improve the overall security and efficacy of your system.

(ii) Mapping - Create a comprehensive inventory or database of all service providers, touchpoints, and third parties involved in collecting, storing, and processing your data. Once mapped, update or amend all agreements with these stakeholders to align with the DPDPA. This ensures transparency and accountability across the entire ecosystem.

(iii) Implementation - Form a dedicated team to manage data classification, tagging, and security across all sources in compliance with the Indian Computer Emergency Response Team (CERT-in) and the ISO 27001 certification (globally recognized standard for information security) requirements. It is important to have measures in place that allow users to withdraw consent easily and without barriers.

(iv) Accountability Protocols - The DPDPA mandates that each consent request be accompanied by clear information for users. This includes: (a) details of the personal data being requested; (b) the purpose of the request; and (c) how the individual can

exercise their rights and seek redressal. For example, even when conducting virtual KYC verification, banks must explain the nature of the data being collected and its intended use. Additionally, implement grievance redressal mechanisms by employing competent professionals.

(v) Audit - Regular internal audits are necessary to ensure the system is functioning effectively and spot potential issues early. Businesses will need to periodically determine whether it qualifies as a "Significant Data Fiduciary" under the DPDPA (Section 10), based on the volume and sensitivity of data processed, risk of harm to consumers, and its impact on national security. If classified as such, additional responsibilities weigh in such as conducting data impact assessments and appointing a Data Protection Officer (DPO) in India.

By proactively ensuring compliance, businesses can be confident of making a smooth transition into a secure data protection environment.

III. Key Sector-Specific Regulations

With the growing concerns around data privacy and protection, various regulatory bodies, such as the Insurance Regulatory and Development Authority of India (IRDAI), the Securities and Exchange Board of India (SEBI), and the Reserve Bank of India (RBI), have implemented their own cybersecurity and data protection guidelines, practices, and frameworks to safeguard sensitive information across different sectors.

1. Securities Sector – The SEBI, by way of a Circular dated August 20, 2024, introduced the Cyber Resilience and Cyber Security Framework (CRCSF), which sets standards and guidelines to strengthen cyber resilience and maintain robust cybersecurity for SEBI-regulated entities. While the SEBI has been issuing frameworks since 2015 to regulate data and cyber security measures for various entities, the August 2024 Circular significantly broadens the scope. It now includes 'Alternate Investment Funds' and adapts to recent technological advancements, replacing all previous SEBI circulars and notifications on this subject.

   The timeline for adopting this framework is as follows:

   a) For previously regulated entities, compliance is required by January 1, 2025; and

   b) For newly regulated entities, the deadline is April 1, 2025.

   The CRCSF takes a graded approach, classifying Regulated Entities (Res) into 5 (five) categories based on operational scope, client base, trade volume, and other criteria. The categories are:

   1. Market Infrastructure Institutions (MII);
   2. Qualified Regulated Entities (Res);
   3. Mid-size Res;
   4. Small-size Res; and
   5. Self-certification Res.

   Additionally, the framework introduces a Cyber Capability Index (CCI) for MIIs and Qualified Res, which assesses their cybersecurity preparedness and resilience based on 23 (twenty three) parameters outlined in Annexure K of the guidelines. MIIs must undergo biannual assessments, while Qualified Res must be assessed annually. All auditors responsible for certifying Cyber Audit Reports under the CRCSF must be empaneled by CERT-In.

   Smaller entities receive certain relaxations but must be affiliated with a Security Operations Centre (SOC), whether it is a market SOC, a group SOC, or a third-party SOC. SOCs play a critical role in monitoring and responding to security threats in real-time, investigating breaches, and determining their root causes. The National Stock Exchange and the Bombay Stock Exchange are required to establish their own Market SOCs by January 1, 2025, and must conduct annual market audits, submitting reports to the SEBI.

   The Circular also outlines clear protocols for vulnerability assessments, penetration testing, audit reporting, recovery planning, and risk classifications. It mandates that all cybersecurity incidents must be reported to CERT-In and the SEBI through email within 6 (six) hours of detection (mkt_incidents@sebi.gov.in) and to the SEBI Incident Reporting Portal within 24 (twenty four) hours. In cases of high or critical incidents, a forensic audit must also be conducted.

2. Insurance Sector - In April 2023, the IRDAI issued the Guidelines on Information and Cyber Security for Insurers. These guidelines aim to prevent accidental or intentional disclosure, alteration, destruction, or misuse of information assets, ensuring a secure cyberspace ecosystem. They apply to all entities regulated by IRDAI, including foreign reinsurance branches and intermediaries. The framework is governed by the Board of Directors, supported by the Risk Management Committee and the Information Security Risk Management Committee (ISRMC). The ISRMC oversees the overall risk management and the Information and Cyber Security Policy.

   It includes officials such as the Chief Risk Officer, Chief Information Security Officer, Chief IT Security Officer, and other key personnel in operations, finance, legal, compliance, and technology roles. The guidelines also mandate an annual Independent Assurance Audit, with the audit report submitted to the IRDAI within 90 (ninety) days of the financial year-end or within 30 (thirty) days of audit completion, whichever is earlier. Importantly, the guidelines enforce data localization, requiring that all ICT infrastructure, critical business data, and sensitive information be stored within India.

3. Reserve Bank of India – The RBI by way of Circular dated November 7, 2023, issued the Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices consolidating all circulars issued on this subject since the year 1998. These Directions are applicable to the following categories:

   1. Banking Companies;
   2. Non-Banking Financial Companies;
   3. Credit Information Companies; and
   4. All India Financial Institutions, such as EXIM Bank, NABARD etc.

These Directions are not applicable to: (i) Local Area Banks; (ii) NBFC Core Investment Companies; and (iii) Base Layer NBFC's.

Key aspects covered by the Master Direction include:

(i) Information Security Policy and Cyber Security Policy;
(ii) Risk Assessment;
(iii) Vulnerability Assessments (VA);
(iv) Controls on teleworking;
(v) Cyber Incident Response and Recovery Management;
(vi) Business Continuity Plan (BCP);
(vii) Disaster Recovery (DR) Policy; and
(viii) Information Systems (IS) Audit.

These Guidelines ensure a robust IT governance framework for the financial sector, emphasizing cybersecurity, risk management, and strategic IT oversight.

IV. Conclusion: Preparing for a Secure Digital Future

The DPDPA marks a crucial turning point in India's approach to data privacy and protection. As businesses prepare to comply with the new legal framework, they must take proactive steps to upgrade their data security, ensure transparency, and meet the expectations set by the DPDPA. With sectoral regulators like the SEBI, IRDAI, and RBI already leading the way, businesses that prioritize compliance will not only safeguard sensitive information but also build trust in an increasingly data-driven world. Preparing for this new era of data protection will ensure businesses stay competitive while maintaining the highest standards of privacy and security.

This newsletter has been contributed by:

Simran Singh, Principal Associate & Megha Chauhan, Senior Associate, Dua Associates, Chandigarh

For further information contact:

Siddhartha Kumar, Partner, Dua Associates, Chandigarh
Email: siddhartha@duaassociates.com

Stay connected with Dua Associates
www.duaassociates.com