INDIALAW

CIVIL

Navigating the Roadmap for DPDP Compliance: What Companies Need to Start On

AUTHOR Appurv Bhatia

PUBLISHED 29 May 2025

The release of the draft Digital Personal Data Protection Rules (DPDP) 2025 by the Ministry of Electronics and Information Technology (MeitY) marks a significant milestone in India's journey toward safeguarding digital privacy. As the regulatory framework evolves, organizations must proactively align their data governance frameworks to meet these upcoming regulations. In an increasingly privacy-conscious market, this is an opportunity to demonstrate a commitment to data protection that goes beyond mere compliance. Adopting best practices in data security and privacy can help businesses differentiate themselves and encourage trust with their customers.

Table of contents

Understanding the DPDP Act and Its Implications

The DPDP Act introduces several key principles that require organizations to rethink their strategies. These include accountability, transparency, data minimization, and proactive risk management. Accountability mandates that organizations take responsibility for the personal data they process, implementing strong governance frameworks and ensuring all employees understand their roles in protecting personal data. Transparency emphasizes clear communication with data principals about how their data is being used. Data minimization encourages collecting only the necessary data for specific purposes, reducing potential exposure in case of a breach. Proactive risk management requires regular assessments of data processing activities and security measures to identify vulnerabilities and implement corrective actions before issues arise.

Key Steps for Companies to Start On

Perform a Gap Assessment of Current Processes and Data vs. the Act

The first step is to conduct a thorough gap assessment to identify discrepancies between current data handling practices and the requirements of the DPDP Act. This involves determining whether your organization falls under the purview of the DPDP Act and identifying your specific obligations as a data fiduciary or data processor. Key considerations include whether your organization processes digital personal data within India or offers goods/services to Indian data principals and identifying your role as a data fiduciary or data processor under the Act.

Identify Tasks with External Implications to Be Actioned Immediately

Companies must prioritize tasks that have immediate external implications, particularly those related to data principal-facing activities. This includes implementing consent management as per DPDPA compliance, ensuring that consent is obtained for each specific purpose of data processing, and that consent requests are not bundled with other terms and conditions. Clear notice and contact information of the data protection officer should be provided, and data principals should be able to easily withdraw consent, with the process being as simple as providing consent. Consent logs must also be retained to demonstrate compliance.

Identify System Changes to Enhance Data Security

Enhancing data security is a critical component of DPDP compliance. Companies should implement advanced data governance measures, including strong data protection strategies and adhering to principles such as data minimization and secure processing. Specific technical and organizational measures include implementing encryption, access controls, and regular security audits. Access to computer resources used by the data fiduciary or data processor should be controlled, and data access should be monitored and logged to detect and address unauthorized access. Companies must also ensure continued data processing in case of data loss or compromise through measures like data backups.

Identify Internal Tasks to Be Completed in Due Course

Internal tasks that need to be completed include conducting data mapping and inventory to have a thorough understanding of data processing activities. This involves identifying and documenting all data processing activities, categorizing data based on sensitivity and purpose, and creating a comprehensive data inventory detailing what data is being collected, where it is stored, and who has access to it. Companies must also establish data lifecycle management practices, deleting personal data once its purpose is fulfilled or upon consent withdrawal, and developing data retention policies addressing different types of data and their respective retention periods. Appointing a Data Protection Officer (DPO) is another crucial internal task, especially for Significant Data Fiduciaries (SDFs) who are required to conduct a data protection impact assessment (DPIA) and audit every 12 months, and submit a report with significant observations to the Board.

Additional Strategic Recommendations

Establish a Strong Incident Response Plan

Organizations should establish a strong and flexible incident response plan that includes triage and documentation systems for rapid breach classification and detailed, real-time documentation. Assigning specific roles to legal, IT, and communications teams can avoid delays during breach response, and conducting periodic breach simulations can validate the plan's effectiveness.

Develop Customizable Breach Notification Templates

Creating tailored templates for various breach types and audiences, such as data principals and the board, ensures clear and actionable information is provided. Data principals should be given clear guidance on steps to protect their data and contact information for inquiries.

Implement Cross-Departmental Collaboration and Staff Training

Forming a cross-departmental breach response team (BRT) with members from IT, legal, and compliance can simplify breach management. Regular training on Rule 7's requirements and breach communication protocols is essential for ongoing compliance.

Strengthen Data Security Infrastructure

Investing in state-of-the-art verification technologies and ensuring compliance with rules through seamless integration with government-issued services like Digital Locker is crucial. Conducting public awareness campaigns to inform parents and guardians about the consent process and how their data is being protected can enhance transparency and trust. Enabling collaboration between government agencies and private entities can ensure a cohesive and user-friendly consent verification process.

Conclusion

Finalisation, notification and implementation of the proposed Digital Personal Data Protection Rules 2025 may be some time away but represent a significant step forward in India's data protection landscape. Compliance builds trust in a data-driven economy. By understanding the prominent features of the DPDP Act, meeting legal compliances, and mitigating data privacy risks from the outset, organizations can avoid penalties and stay ahead of the competition. The journey to compliance requires a structured approach, proactive engagement, and a commitment to continuous improvement. As the regulatory environment evolves, companies must remain vigilant and adapt their strategies to ensure the protection of personal data and the rights of data principals.

For further details write to contact@indialaw.in

Related Practice Areas

Data Protection and Privacy