ECONOMIC LAWS PRACTICE
ADVOCATES & SOLICITORS

KEY HIGHLIGHTS OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025

I. KEY HIGHLIGHTS OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025

The Digital Personal Data Protection (DPDP) Rules, 2025, recently released by the Ministry of Electronics and Information Technology **(MeitY)**, operationalize the DPDP Act, 2023, by providing actionable guidance on critical aspects such as data processing, consent management, breach notifications, and cross-border transfers. The draft Rules are a significant step toward building a robust data protection framework in India and are currently open for public consultation until February 18, 2025. This is a vital opportunity for stakeholders to ensure the framework is both practical and forward-looking.

Consent Mechanisms

Consent remains the bedrock of the DPDP Rules, emphasizing transparency and ease for Data Principals (individuals).

- ***Informed Consent:*** Data Fiduciaries must obtain clear, specific, and informed consent from Data Principals. Consent notices should outline the purpose and categories of personal data being collected in simple, accessible language.
- ***Simplified Withdrawal:*** Withdrawing consent must be as seamless as giving it. Fiduciaries are required to establish user-friendly mechanisms for revoking consent at any time.
- ***Consent Managers:*** These intermediaries manage consent transactions between Fiduciaries and Principals. Consent Managers must:
  - Register with the Data Protection Board **(DPB)**.
  - Ensure that their systems are secure, transparent, and unbiased.
  - Maintain independence to avoid conflicts of interest with Fiduciaries.

Obligations of Data Fiduciaries:

The Rules impose strict obligations on Data Fiduciaries to ensure data security and integrity.

- ***Security Safeguards:*** Fiduciaries must implement encryption, access controls, and other technical measures to prevent unauthorized data access or breaches.
- ***Audit Trails:*** Logs of data access and usage must be maintained for at least one year to enable accountability and traceability.
- ***Minimization of Data:*** Personal data must only be collected and processed to the extent necessary for the specified purpose.

Breach Notification & Management:

Addressing data breaches promptly is a key focus.

- ***Timelines for Notification:*** Fiduciaries must inform the DPB of any breach within 72 hours of becoming aware of the incident.

- ***Information to Affected Individuals:*** Data Principals must be notified of breaches that could cause significant harm, detailing the nature of the breach and recommended mitigation steps.

Cross-Border Data Transfers:

- ***Permissibility:*** Transfer of personal data outside India are allowed, subject to specific conditions ensuring that the recipient country or organization provides an adequate level of protection as determined by the Central Government.
- ***Strategic Balancing:*** While enabling international data flows, the Rules maintain safeguards to prevent misuse and protect national interests.

Special Provisions for Children's Data:

- ***Parental Consent:*** Processing the personal data of children (individuals under 18 years) requires verifiable parental or guardian consent.
- ***Prohibited Activities:*** Data Fiduciaries are restricted from using children's data for profiling, behavioral tracking, or any purposes detrimental to their welfare.
- ***Age Verification Mechanisms:*** Fiduciaries must implement reliable systems to verify the age of individuals and ensure compliance with child-specific provisions.

Rights of Data Principals:

The DPDP Rules empower Data Principals with several rights to exercise control over their personal data:

- ***Right to Access:*** Individuals can request information on the data collected and processed about them.
- ***Right to Correction and Erasure:*** Data Principals have the right to request corrections to inaccurate data or deletion of data no longer required.
- ***Right to Nominate:*** Principals can appoint representatives to exercise these rights on their behalf.

The Data Protection Board (DPB):

The DPB will function as the regulatory body overseeing compliance with the DPDP framework:

- ***Adjudicatory role:*** It will address grievances, monitor compliance, and impose penalties for violations.
- ***Digital-First Approach:*** The DPB is designed as a digital-first entity to streamline dispute resolution and enforcement.

II. WELCOME CLARIFICATIONS AND POTENTIAL PITFALLS/LACUNAE OF THE DPDP RULES, 2025

Welcome Clarifications:

- ***Enhanced Transparency and Accountability:*** The Rules establish clear guidelines for consent, security, and breach management, ensuring accountability for Data Fiduciaries.
- ***Flexibility for Cross- Border Transfers:*** The pragmatic stance on data transfers promotes global interoperability while safeguarding domestic interests.
- ***Protection of Vulnerable Groups:*** Provisions related to children's data reflect a strong focus on safeguarding the rights of minors.
- ***Empowerment of Data Principals:*** The Rules provide individuals with actionable rights to access, correct, and delete their personal data.

Potential Pitfalls/Lacunae:

- ***Complex Compliance Requirements:*** Small and Small and medium enterprises (SMEs) may face challenges in implementing the advanced security measures and consent frameworks required.
- ***Potential Overreporting of Breaches:*** The obligation to notify the DPB and affected individuals for all breaches could overwhelm regulatory systems and reduce focus on critical incidents.
- ***Ambiguities in Enforcement:*** Certain aspects, such as the role and accountability of Consent Managers, require further clarification to avoid gaps in implementation.
- ***Burden on Parental Verification:*** The stringent requirements for processing children's data could create logistical hurdles for Data Fiduciaries.

III. PUBLIC CONSULTATION: AN OPPORTUNITY FOR REFINEMENT

The draft Rules are open for public feedback, with stakeholders encouraged to submit their views by February 18, 2025. Key areas for input include:

- Streamlining compliance requirements for SMEs.
- Refining breach notification thresholds to focus on significant incidents.
- Clarifying cross-border transfer mechanisms and adequacy assessments.
- Defining the scope and liabilities of Consent Managers.

IV. CONCLUSION

ELP Comments

The The Digital Personal Data Protection (DPDP) Rules, 2025, represent a pivotal milestone in India's journey toward a robust data protection regime. While they align with global best practices, their practical implementation will depend on addressing key stakeholder concerns during the consultation process. Active engagement is essential to create a framework that balances individual privacy rights with business innovation.

Provisions related to the Data Protection Board (Rules 16-20) will be effective upon official notification. Operational requirements (Rules 3-15, 21, and 22) will be implemented later, though no specific timeline has been provided. This phased approach aims to give businesses time to adjust their operations, but clarity on timelines is essential for preparation.

We trust you will find this an interesting read. For any queries or comments on this update, please feel free to contact us at insights@elp-in.com or write to our authors:

Vinay Butani, Partner- *VinayButani@elp-in.com*