



EXAMINING THE DRAFT RULES OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Draft Rules issued on January 3, 2025, by the Ministry of Electronics and Information Technology (MeitY) aim to operationalize the Digital Personal Data Protection Act, 2023 (**'DPDP Act'**). These rules set out the detailed mechanisms, rights, duties, and compliance standards to ensure effective implementation of the DPDP Act. Public comments are invited on these draft rules until February 18, 2025, via the MyGov portal.

A. KEY PROVISIONS OF THE DRAFT RULES

a) **Title and Applicability**

- The rules are referred to as the “Digital Personal Data Protection Rules, 2025” (the **'Rules'**).
- Sections 3-15, 21, and 22 will take effect on a date specified by the Central Government.

b) **Definitions and Clarifications**

- The rules adopt definitions from the DPDP Act, including terms like “data fiduciary,” “data principal,” and “consent manager.”

c) **Obligations of Data Fiduciaries**

- Notification to Data Principals: Data fiduciaries are required to issue clear, concise, and intelligible notices about the collection and processing of personal data. Notices must include details of the data being processed and the purpose.
- Security Measures: Data fiduciaries must implement adequate technical and organizational measures, such as encryption, access control, and regular audits, to safeguard personal data.
- Reporting Data Breaches: In case of a data breach, fiduciaries must notify affected data principals and the Data Protection Board within 72 hours.

d) **Consent Management**

- Consent managers are intermediaries to facilitate consent-based data processing.
- They must adhere to strict operational and technical standards.

e) **Rights of Data Principals**

- Data principals have the right to access, correct, or delete their personal data. The rules mandate that data fiduciaries must facilitate these rights through their platforms.

f) **Processing of Children's Data**

- For minors, consent must be verifiable and obtained from parents or lawful guardians. Special care is to be taken to ensure the legitimacy of the guardian's consent.



- g) **Exemptions for State Entities**
 - State agencies are permitted to process personal data without consent in specified situations, such as providing benefits or services, subject to compliance with standards outlined in the rules.
- h) **Cross-Border Data Transfers**
 - Personal data may be transferred outside India, provided the destination country meets criteria specified by the Central Government.
- i) **Responsibilities of Significant Data Fiduciaries (SDFs)**
 - Entities meeting thresholds (e.g., volume of data, sensitivity, or processing impact) are classified as SDFs.
 - SDFs must conduct annual data protection impact assessments and submit audit reports.
- j) **Penal Provisions**
 - Non-compliance with the rules can attract penalties as per the DPDP Act.

B. IMPLEMENTATION FRAMEWORK

- a) **Data Protection Board of India:** The board will act as the regulatory authority for monitoring compliance, addressing grievances, and penalizing non-compliance. The rules provide details about its composition, roles, and functions.
- b) **Appeals Process:** Aggrieved parties can appeal decisions of the Data Protection Board to an Appellate Tribunal. Digital filing and resolution mechanisms are emphasized.
- c) **Governance Mechanisms:** Provisions for regular audits, stakeholder consultations, and clear reporting obligations have been included to enhance transparency and accountability.

C. COMPLIANCE BY PRIVATE COMPANIES

- a) **Data Fiduciary Responsibilities**
 - Notices: Provide data principals with clear, comprehensible notices detailing the data processing purpose and type of data collected.
 - Consent: Obtain, record, and manage explicit consent from data principals using approved consent mechanisms.
- b) **Data Security and Breach Notification**
 - Implement advanced security measures such as encryption, access control, and regular monitoring.
 - Notify the Data Protection Board and affected individuals within 72 hours of a data breach.



- c) **Rights Facilitation for Data Principals**
 - Create user-friendly systems to allow individuals to access, correct, or delete their data.
- d) **Compliance for Significant Data Fiduciaries**
 - Conduct annual data protection impact assessments and audits.
 - Designate a Data Protection Officer (DPO) and establish grievance redressal mechanisms.
- e) **Children's Data Processing**
 - Verify parental consent for processing children's data using government-approved methods.
- f) **Cross-Border Data Transfers**
 - Ensure compliance with government-specified safeguards for transferring personal data outside India.
- g) **Records Maintenance**
 - Maintain detailed records of consent, data processing activities, and data sharing for specified durations.
- h) **Capacity Building**
 - Train employees on data protection principles and practices.
 - Develop a dedicated team or hire external consultants to manage compliance.
- i) **Infrastructure Development**
 - Implement IT systems for data encryption, anonymization, and access controls.
 - Invest in secure storage solutions to prevent data breaches.
- j) **Policy Updates**
 - Revise privacy policies and terms of service to align with the rules.
 - Establish mechanisms to handle data principal rights requests.
- k) **Consent Management**
 - Utilize consent management platforms to obtain, manage, and withdraw consent efficiently.
- l) **Collaborate with Regulators**
 - Engage with government bodies and industry associations to understand compliance expectations.



D. POTENTIAL CHALLENGES AND IMPLICATIONS FOR PRIVATE COMPANIES

CHALLENGES

- a) **Exemptions to State Entities:** Uneven compliance obligations could place private entities at a competitive disadvantage.
- b) **Ambiguity in Transfer Rules:** Uncertainty regarding cross-border data transfer criteria could disrupt international business operations.
- c) **Burden on SMEs:** High compliance costs and technical requirements could disproportionately affect small businesses.
- d) **Short Timelines for Breach Notifications:** The 72-hour requirement may not provide adequate time for proper investigation and reporting.
- e) **Vague SDF Classification:** Criteria for classifying entities as SDFs lack clarity, leading to potential overreach.
- f) **Overlapping Regulations:** Potential conflicts with existing sector-specific data laws.

IMPLICATIONS

- a) **Compliance Costs:** Companies must invest in consent management systems, secure IT infrastructure, and data protection audits.
- b) **Operational Adjustments:** Businesses may need to redesign processes to accommodate data portability, correction, and deletion requests.
- c) **Global Operations:** Restrictions on cross-border data flows could affect companies with international operations, requiring additional resources to comply with transfer regulations.
- d) **Risk of Penalties:** Non-compliance can lead to significant penalties, affecting financial and reputational stability.



E. DIFFICULTIES ARISING FROM DRAFT DPDP RULES

The **Rules** present several challenges that are not specific to any single sector but instead arise from their general nature and implications. Below are some key challenges:

A. Ambiguity in Key Definitions

- Lack of Clarity: Terms like "consent manager," "reasonable purposes," and "public interest" are not clearly defined, leading to potential misinterpretations and inconsistent applications across sectors.
- Overbroad Interpretation: Vague definitions can allow for expansive interpretations, creating uncertainty for individuals and organizations.

B. Enforcement and Oversight

- Data Protection Board (DPB): The rules propose the establishment of a DPB but lack details about its independence, resources, and operational framework.
- Fragmented Implementation: Without clear roles and responsibilities, ensuring uniform compliance and enforcement could be challenging.

C. Consent Management Complexity

- Granularity of Consent: Requiring explicit, informed, and specific consent for every use of data can burden users with repeated requests and lead to "consent fatigue."
- Tech Burden: Organizations will need significant investments in systems for managing consent effectively, which may disadvantage smaller entities.

D. Data Localization Requirements

- Global Operations Impact: Implicit expectations for storing and processing data locally could disrupt cross-border operations and increase costs.
- Conflict with Global Standards: Potential conflicts with international frameworks can complicate compliance for multinational organizations.

E. Broad Exemptions for the Government

- Lack of Checks: The government's ability to exempt itself from certain provisions under the guise of national security or public interest may lead to misuse or abuse of power.
- Transparency Concerns: Absence of robust oversight mechanisms for exemptions undermines accountability.

F. Data Breach Notification Challenges

- Unrealistic Timelines: Short timelines for notifying the authorities of data breaches might be impractical, especially for complex incidents requiring forensic analysis.
- Ambiguity in Reporting: Lack of clarity on what constitutes a "significant" breach adds to compliance challenges.

G. Impact on Small and Medium Enterprises (SMEs)

- Compliance Costs: The financial and administrative burden of adhering to the rules can disproportionately affect SMEs.
- Lack of Guidance: Limited sector-agnostic guidelines for SMEs to understand and implement compliance measures.

H. Cross-Border Data Transfers

- Uncertain Mechanism: While the rules mention cross-border data transfers to "trusted" jurisdictions, the criteria for trustworthiness are vague.
- Operational Hurdles: Businesses relying on global data flows face uncertainty in managing international operations.

I. Lack of User Awareness

- Low Digital Literacy: Many users lack awareness or understanding of data protection principles, leading to potential misuse of personal data despite regulatory safeguards.
- Responsibility Mismatch: Over-reliance on user consent assumes that individuals fully comprehend the implications of sharing their data.

J. Balancing Privacy and Innovation

- Chilling Effect: Overregulation or overly restrictive data usage rules could stifle innovation, particularly in AI, machine learning, and data-driven sectors.
- Inequity in Impact: Larger corporations with better resources may adapt more easily than startups, exacerbating market imbalances.

K. Lack of Sector-Specific Nuance

- One-Size-Fits-All Approach: The rules lack differentiation based on the sensitivity of data or sector-specific needs, which may lead to disproportionate compliance burdens.

L. Legal Uncertainty and Litigation

- Interpretational Variances: The ambiguities in the rules could lead to a surge in litigation as stakeholders contest interpretations.
- Overlapping Jurisdictions: Potential overlaps with existing laws (e.g., IT Act, Consumer Protection Act) could create legal conflicts.

CONCLUSION

The Rules under the DPDP Act aim to establish a robust framework for data protection and privacy in India. They emphasize safeguarding personal data, ensuring transparency, and empowering data principals. By introducing consent management systems, mechanisms for addressing data breaches, and compliance audits for significant data fiduciaries, the rules reflect a comprehensive approach to modern data governance.



The Rules represent a landmark step toward strengthening data protection in India. While they establish a comprehensive framework for accountability and transparency, significant challenges remain, particularly for private entities.

Following are the indicative points summarizing the path forward:

- **Clarity and Precision:** The Rules must define key terms and concepts more clearly to reduce ambiguity and ensure consistent interpretation.
- **Balanced Regulation:** A tailored approach that considers the needs of different sectors and organizational sizes can help avoid disproportionate compliance burdens.
- **Enforcement and Accountability:** Strengthening the independence and operational framework of the Data Protection Board (DPB) is essential for fair and effective enforcement.
- **Global Alignment:** Harmonizing rules with international data protection standards can facilitate seamless cross-border operations.
- **Stakeholder Collaboration:** Engaging industry, civil society, and government stakeholders can ensure that the rules are practical and inclusive.
- **Phased Implementation:** Advocate for phased implementation timelines to allow companies to align operations without disrupting existing services.

By addressing these challenges, the DPDP Rules can achieve their dual objectives of safeguarding personal data and fostering innovation, paving the way for a secure and thriving digital ecosystem. These efforts can create a balanced ecosystem that upholds privacy rights while fostering innovation and economic growth.

Further, by advocating for sector-specific adaptations and investing in compliance systems, the automotive sector can align with the new regulations without compromising operational efficiency or technological advancement.

Disclaimer:

This article is intended for informational purposes only and does not constitute legal advice. While every effort has been made to ensure the accuracy of the information provided, readers are advised to consult authoritative sources for specific guidance on the Digital Personal Data Protection Act, 2023 and its draft rules. The opinions expressed are those of the author and do not necessarily reflect the views of any organization.