KOCHHAR & CO.
ADVOCATES & LEGAL CONSULTANTS

Digital Personal Data Protection Rules, 2025: Strengthening India's Data Protection Framework

The Ministry of Electronics and Information Technology has unveiled the draft Digital Personal Data Protection ("**DPDP**") Rules, 2025, emphasizing user rights, Data Fiduciaries' obligations, and robust safeguards for personal information. These rules, designed to enforce the DPDP Act, 2023, reflect India's commitment to establishing a comprehensive data protection regime. While they aim to enhance transparency and accountability, businesses face the challenge of aligning compliance with operational feasibility. Public consultation on the draft rules until February 18, 2025, presents an opportunity for stakeholders to shape the future of India's digital data ecosystem.

Key Stakeholders of the DPDP Framework:

1. Data Principals: Individuals whose personal data is collected, processed, or stored, with rights to provide consent, withdraw consent, access, or erase their data are the heart of the DPDP Framework, known as Data Principals. They can lodge complaints with the Data Protection Board if their rights under the law are violated.

2. Data Fiduciaries: Entities (businesses, organizations, or government agencies) responsible for collecting and processing personal data are categorised as Data Fiduciaries. They are obligated to ensure transparency, security, and data retention compliance, while addressing grievances within specified timelines.

3. Consent Managers: Registered intermediaries facilitating consent collection and withdrawal for Data Principals known as Consent Managers are required to act in a fiduciary capacity to implement adequate security measures to prevent unauthorized access to consent records. Consent Managers must adhere to strict financial, technical, and operational criteria, and maintain strict confidentiality. The entity must have a minimum net worth of INR 2 (two) crore to demonstrate financial stability. The platform used by the Consent Manager must be interoperable, certified to allow seamless data transfer and consent management across multiple Data Fiduciaries.

4. Minors and Persons with Disabilities: Special categories requiring additional protections, such as verifiable parental/guardian consent for minors and accessible systems for persons with disabilities are identified in the DPDP Framework.

5. Data Protection Board: A regulatory authority under the DPDP Act, 2023, the Data Protection Board is responsible for ensuring compliance with data protection laws, addressing grievances, managing data breach notifications from Data Fiduciaries, and enforcing penalties for violations.

Obligations of Data Fiduciaries:

1. Transparency and Consent: Data Fiduciaries are obligated to provide clear, itemized notices to Data Principals before collecting data and obtain their informed consent.

2. Data Minimization: Data Fiduciaries must collect and process only the personal data necessary for the specific purpose for which it is required.

3. Security Safeguards: Data Fiduciaries are required to implement robust security measures, such as encryption and masking, to protect personal data from breaches or unauthorized access.

4. Breach Notification: Data Fiduciaries must notify affected Data Principals and the Data Protection Board of any data breaches within 72 hours, including details of the breach and remedial measures undertaken.

5. Retention and Erasure: Data Fiduciaries are obligated to retain personal data and maintain backups for a period of one year to prevent breaches. However, they must ensure the data is stored only as long as necessary for the stated purpose and promptly erase it once it is no longer required, unless its retention is mandated by law.

6. Data Access Rights: Data Fiduciaries must provide mechanisms for Data Principals to access, correct, or erase their personal data upon request.

7. Grievance Redressal: Data Fiduciaries are required to establish a grievance redressal mechanism to address complaints from Data Principals within a defined timeline.

8. Appointment of Officers: Data Fiduciaries must appoint a Data Protection Officer ("**DPO**") to oversee compliance with the DPDP Act, 2023 and manage data protection processes.

9. Data Audits: Data Fiduciaries are obligated to appoint DPOs, conduct regular audits and data protection impact assessments to ensure adherence to the provisions of the DPDP Act, 2023.

10. Special Provisions for Minors and Persons with Disability
    Data Fiduciaries must obtain verifiable parental consent before processing the personal data of minors and are prohibited from engaging in tracking,

behavioural monitoring, or targeted advertising towards them. Likewise for persons with disabilities, consent must be obtained from legally recognized guardians. The DPDP Rules, 2025 state that data processing with respect to children may not be restricted when data processed relate to protecting children's health or ensuring public safety in educational or healthcare settings or for archival, research, or statistical purposes, adhering to specified standards.

Other Notable Provisions:

Significant Data Fiduciaries (handling large-scale sensitive data) shall additionally be responsible for conducting annual Data Protection Impact Assessments and shall be prohibited from making cross-border transfers of specified personal data without central government approval.

Significant Data Fiduciaries have been segregated into E-commerce platforms (not less than 2 (two) crore registered users), online gaming platforms (not less than 50 (fifty) lakh registered users) and social media intermediaries (not less than 2 (two) crore registered users), with significant user bases in India and are required to erase personal data of users 3 (three) years after it is no longer needed.

Key Takeaways:

1. Clear and Comprehensive Notices: Data Fiduciaries must provide clear and easily understandable notices to Data Principals, detailing the types of data collected, its processing purposes, and users' rights.

2. Data Minimization: Personal data collection and processing must be limited to what is strictly necessary to achieve the specified purposes.

3. Parental Consent for Minors: Data Fiduciaries must obtain verifiable parental consent before processing the personal data of minors, ensuring adequate safeguards for children's data.

4. Right to Information: Data Principals can request access to their personal data and its processing details from Data Fiduciaries.

5. Data Breach Notifications: Data Fiduciaries are obligated to notify affected individuals and the government of any data breaches promptly, including details on the breach's scope and mitigation measures.

6. Data Retention Policy: Personal data must be erased when it is no longer required for its original purpose, except when required for legal compliance. Before erasing personal data, the Data Fiduciary must notify the Data Principal at least 48 hours in advance, allowing the Dara Principal adequate time to take necessary actions if needed.

7. Data Transfers Abroad: Transfers of personal data outside India are subject to government-approved safeguards and permissions to ensure national security and individual privacy.

8. Accountability and Audits: Data Fiduciaries categorized as significant must conduct periodic data protection impact assessments and audits to comply with the DPDP Act, 2023.

9. Grievance Redressal: Data Fiduciaries must establish mechanisms to address grievances from Data Principals efficiently and transparently.

10. Sanctions for Non-Compliance: Non-compliance with the DPDP Rules, 2025 will attract huge penalties, reinforcing the emphasis on fiduciary responsibility and accountability.

Next Steps:

Businesses are advised to adopt measures by conducting a compliance gap analysis to identify risks. In addition to drafting or updating privacy policies and contracts to align with the DPDP Rules, 2025 businesses shall be required to adopt tools for automated compliance monitoring, consent management, and data security. It will be equally important to educate employees and partners about new responsibilities.

Conclusion:

The DPDP Rules, 2025 represent a significant milestone in India's journey toward a robust data protection regime. While they establish crucial safeguards for digital data, gaps remain, such as the impracticality of consent in certain scenarios and the ambiguity surrounding cross-border data transfers, which may create challenges for globally operating businesses. Addressing these concerns through public consultation and targeted refinements will be essential for achieving a balanced framework. For businesses, this is an opportunity to strengthen data protection practices, foster trust, and align with evolving regulatory standards.