Summary - Digital Personal Data Protection (DPDP) Rules, 2025

The Government of India on 14th November 2025 has notified the Digital Personal Data Protection Rules, 2025 (DPDP Rules) to operationalize the Digital Personal Data Protection Act, 2023 (DPDP Act), an Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto. Lawful purpose means any purpose which is not expressly forbidden by law. **The Rules introduce an eighteen-month period for phased compliance**.

The legal framework is founded on seven fundamental principles. These principles encompass consent and transparency, purpose limitation, data minimization, accuracy, storage limitation, security measures, and accountability.

The Provisions of the Act shall apply to the processing of digital personal data within the territory of India where the personal data is collected:

- ✓ in digital form; or
- ✓ in non-digital form and digitised subsequently.

Also applies to the processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to the offering of goods or services to Data Principals within the territory of India.

The provision of the Act shall not apply to:

- ✓ Personal data processed by an individual for any personal or domestic purpose; and
- ✓ Personal data that is made or caused to be made publicly available by the Data Principal to whom such personal data relates or any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

Key terms under the DPDP Act:

Data Fiduciary: Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

Data Principal: The individual to whom the personal data relates. In the case of a child, this includes a parent or lawful guardian. For a person with a disability who cannot act independently, this includes the lawful guardian acting on their behalf.

Data Processor: Any entity that processes personal data on behalf of a Data Fiduciary.

Digital personal data: Personal data in digital form.

Personal data: Any data about an individual who is identifiable by or in relation to such data.

Personal data breach: Any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data that compromises the confidentiality, integrity or availability of personal data.

Other key features:

Data Protection Board of India:

The Central Government shall establish, for the purposes of this Act, a Board to be called the Data Protection Board of India. The Board functions as an independent body that oversees compliance, investigates breaches, and ensures that corrective measures are taken. It plays a key role in enforcing the rights granted under the Act and maintaining trust in the system.

Consent-based processing:

Processing of personal data is allowed only with valid, informed, and free consent of the individual (data principal). Individuals may withdraw their consent at any time. Citizens can seek information on what personal data has been collected, why it was collected, and how it is being used. Organisations must provide this information in a simple form. Individuals can ask for a copy of their personal data that is held by a Data Fiduciary.

Transparency and Accountability Measures:

The Regulations mandate that each Data Fiduciary provide explicit contact details for inquiries concerning personal data. This could involve the contact information of a designated officer or a Data Protection Officer. Major Data Fiduciaries are subject to more rigorous obligations. They are required to perform independent audits and execute impact assessments. Additionally, they must adhere to more stringent evaluations when employing new or sensitive technologies. In certain instances, they are obligated to comply with governmental directives regarding restricted data categories, including local storage when necessary.

Personal Data Breach Notification:

When a breach takes place, the Data Fiduciary must inform all affected individuals without delay. The message must be in plain language and must explain what happened, the possible impact, and the steps taken to address the issue. It must also include contact details for help.

Rights of the Data Principal:

Individuals can ask to access their personal data or seek corrections and updates. They may also request the removal of data in certain situations. They can authorise someone else to exercise these rights on their behalf. Data Fiduciaries must respond to such requests within ninety days. Every person has the choice to allow or deny the use of their personal data.

Penalties:

The DPDP Act imposes substantial financial penalties for non-compliance by Data Fiduciaries. The highest penalty, up to ₹250 crore, applies to the failure of a Data Fiduciary to maintain reasonable security safeguards. Failing to notify the Board or affected individuals of a personal data breach, as well as violating obligations related to children, can each attract penalties of up to ₹200 crore. Any other violation of the Act or Rules by a Data Fiduciary may result in penalties of up to ₹50 crore.

Phased Enforcement:

Certain provisions of the Act concerning the Data Protection Board will take effect from 14th November 2025, which is the date of publication. Other provisions of the Act related to notifying the data principal by the data fiduciary, safeguarding personal data (security measures), informing about data breaches, the retention period for data, disclosing the details of the data protection officer, obtaining consent from the data principal, and the rights of the data principal, among others, will come into effect **eighteen months** following the publication date of this gazette.

Conclusion:

The DPDP framework places the individual at the centre of India's data protection system. It aims to give every citizen clear control over personal data and confidence that it is being handled with care. The rules are written in plain language, making it easy for people to understand their rights without difficulty. They also ensure that organisations act responsibly and remain accountable for how they use personal data.