

Digital Personal Data Protection Act (DPDP), 2023: Reference Guide

1. Introduction and Scope

The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's primary legislation governing the processing of digital personal data. It balances the rights of individuals to protect their data with the need for organizations to process data for lawful purposes.

1.1 Applicability

- **Digital Data:** Applies to personal data collected in digital form or non-digital data that is subsequently digitized.
- **Territorial Scope:** Applies to processing within India. It also applies to processing outside India if it involves offering goods or services to individuals in India.
- **Exclusions:** Does not apply to personal data processed by an individual for personal or domestic purposes.

2. Key Definitions

- **Data Principal:** The individual to whom the personal data relates (e.g., an employee or customer).
- **Data Fiduciary:** The entity (company/employer) that determines the purpose and means of data processing.
- **Data Processor:** Any person or entity that processes data on behalf of a Data Fiduciary.
- **Personal Data:** Any data about an individual who is identifiable by or in relation to such data.

3. Grounds for Processing

Personal data may only be processed for a lawful purpose under two conditions:

1. **Consent:** The individual has given free, specific, informed, and unconditional consent.
2. **Certain Legitimate Uses:** Processing is allowed without consent for specific cases like medical emergencies, disasters, or employment-related purposes.

4. Rights of the Data Principal

- **Right to Information:** To know what data is being processed and with whom it is shared.
- **Right to Correction and Erasure:** To update inaccurate data or request deletion once the purpose is served.
- **Right of Grievance Redressal:** To complain to the Data Fiduciary or the Data Protection Board.
- **Right to Nominate:** To appoint a person to exercise rights in case of death or incapacity.

5. Obligations of Data Fiduciaries

- **Notice:** A clear notice must be provided before or at the time of seeking consent.
- **Accuracy:** Ensure personal data is accurate and complete.
- **Security Safeguards:** Implement reasonable security measures to prevent data breaches.
- **Breach Notification:** Inform the Data Protection Board and affected individuals in case of a data breach.
- **Data Erasure:** Delete data as soon as the purpose of collection is fulfilled.

6. Penalties for Non-Compliance

The Act specifies heavy financial penalties for violations:

- **Failure to prevent data breaches:** Up to ₹250 Crore.
- **Failure to notify a breach:** Up to ₹200 Crore.
- **Non-fulfillment of obligations for children's data:** Up to ₹200 Crore.
- **Breach of duties by Data Principals:** Up to ₹10,000.