BLOGS

Key Concepts of the Digital Personal Data Protection Act (DPDP Act), 2023

Khushi Malviya · 21 Jul 2025

Introduction

In an increasingly data-driven world, safeguarding personal information has become a top priority. To address these concerns, India introduced the Digital Personal Data Protection (DPDP) Act, 2023, marking a significant milestone in the country's approach to data privacy and protection. This legislation lays the foundation for a framework that ensures accountability, transparency, and fairness in the processing of digital personal data.

Scope and Applicability

The DPDP Act applies to:

- The processing of digital personal data within India, regardless of whether the processing takes place in India or not.
- Data processed outside India if it involves offering goods or services to individuals in India.

This extraterritorial application ensures that global companies handling Indian user data remain within the purview of the Act.

The Act focuses **exclusively on digital personal data**, excluding non-digitized formats. "Personal data" is defined as any data about an individual who is identifiable from such data.

This clear digital boundary distinguishes the DPDP Act from broader global laws like the GDPR, streamlining its enforcement in India's digital ecosystem.

Foundational Concepts

The Act is built upon several core ideas that define its scope and application:

- Personal Data: This is the central subject matter of the Act. It is defined as “any data about an individual who is identifiable by or in relation to such data.” This broad definition covers any information that can directly or indirectly identify a person, whether online or offline, as long as it is in digital form or digitised subsequently.The Act applies to the processing of digital personal data within India and, under certain conditions, to processing outside India if it involves offering goods or services to Data Principals in India.
- Processing: The Act defines processing comprehensively as “an operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.” Essentially, any action taken with digital personal data falls under this definition.

Key Players Under the DPDP Act

The Act identifies specific roles and responsibilities for entities involved in data processing:

- Data Principal: This is the individual to whom the personal data relates. The Act is designed to protect the rights of the Data Principal. They are the owners of their personal data and have specific rights granted under the Act.
- Data Fiduciary: This is the entity (person, company, firm, state, etc.) who “determines the purpose and means of processing of personal data.” The Data Fiduciary is the primary duty-holder under the Act, responsible for complying with its provisions regarding the personal data they process. Think of them as the decision-makers regarding why and how data is processed.
- Data Processor: This is an entity that “processes personal data on behalf of a Data Fiduciary.” Data Processors act under the instructions of the Data Fiduciary. While the primary obligations lie with the Data Fiduciary, the Act also imposes certain duties on Data Processors, particularly regarding security safeguards.
- Significant Data Fiduciary: The Central Government may notify certain Data Fiduciaries as ‘Significant Data Fiduciaries’ based on factors such as the volume and sensitivity of personal data processed, the risk of harm to the Data Principal, and the potential impact on the sovereignty and integrity of India. Significant Data Fiduciaries have additional obligations, including appointing a Data Protection Officer and conducting Data Protection Impact

Assessments.

Principles of Data Processing

The Act is grounded in principles that govern how data should be processed:

- Consent: A cornerstone of the Act. Personal data can generally only be processed for a lawful purpose after obtaining the consent of the Data Principal. Consent must be free, specific, informed, unconditional, and unambiguous, with a clear affirmative action. The Data Principal has the right to withdraw consent at any time.
- Lawful Purpose: Processing must be for a purpose that is not prohibited by law. The purpose for which data is collected must be clearly stated to the Data Principal.
- Legitimate Uses: The Act also permits processing of personal data without consent in certain specified circumstances, referred to as “legitimate uses.” These include processing for purposes such as:
  - For the performance of any function under any law or for the exercise of any sovereign function.
  - For the performance by the State or any of its instrumentalities of any function under any law.
  - For fulfilling any legal obligation.
  - For responding to a medical emergency.
  - For taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health.
  - For purposes of employment.
  - In the public interest (as may be prescribed).
- Purpose Limitation: Personal data can only be used for the specific purpose for which consent was obtained or for a legitimate use. It cannot be repurposed for other uses without fresh consent or another legitimate basis.
- Data Minimisation: Data Fiduciaries must only collect and process personal data that is necessary for the specified lawful purpose. Excessive data collection is to be avoided.
- Accuracy: Data Fiduciaries must make reasonable efforts to ensure that the personal data being processed is accurate and complete.

- Storage Limitation: Personal data must be retained only for as long as is necessary for the purpose for which it was processed, unless retention is required by law.

Obligations of Data Fiduciaries

The Act imposes significant obligations on Data Fiduciaries:

- Notice: Data Fiduciaries must provide a clear and itemised notice to the Data Principal before or at the time of requesting consent. This notice must inform the Data Principal about the personal data to be collected, the purpose of processing, and how they can exercise their rights.
- Security Safeguards: Data Fiduciaries must implement reasonable security safeguards to prevent personal data breaches. This includes technical and organisational measures.
- Data Breach Notification: In the event of a personal data breach, the Data Fiduciary must notify the Data Protection Board of India and affected Data Principals in a timely manner. A “personal data breach” is defined as any unauthorised processing of personal data that compromises its confidentiality, integrity, or availability.
- Grievance Redressal Mechanism: Data Fiduciaries must establish a mechanism for the redressal of grievances of Data Principals.

Rights of Data Principals

The Act empowers Data Principals with several rights:

- Right to Access Information: The right to obtain from the Data Fiduciary a summary of personal data being processed, the processing activities, and the identities of the Data Fiduciary and Data Processors.
- Right to Correction and Erasure: The right to seek correction, completion, updating, and erasure of their personal data.
- Right to Grievance Redressal: The right to a readily available grievance redressal mechanism provided by the Data Fiduciary.
- Right to Nominate: The right to nominate another person who shall exercise their rights under the Act in the event of their death or incapacity.

Cross-Border Data Transfers

The Act permits the transfer of personal data outside India to certain countries or territories as may be notified by the Central Government. Such transfers must still adhere to the obligations and conditions specified under the Act.

Exemptions under the Act

The Act provides for certain exemptions from its applicability, including:

- Processing of personal data for preventing and investigating any offence.
- Processing necessary for enforcing any legal right or claim.
- Processing by the State or its instrumentalities for matters related to the security of the State, public order, or preventing incitement to commit any cognizable offence relating to the sovereignty and integrity of India.
- Processing of personal data that is necessary for research, archiving, or statistical purposes, provided the data is not used to take any decision specific to a Data Principal and is processed in accordance with prescribed standards.

Enforcement and Penalties

The Act establishes the **Data Protection Board of India** as the independent body responsible for enforcing the Act, inquiring into breaches, and imposing penalties. The Act specifies significant penalties for non-compliance, which can be imposed on Data Fiduciaries or Data Processors based on the nature and severity of the contravention.

Conclusion

The DPDP Act, 2023 marks a transformative step in India’s digital governance by emphasizing user consent, transparency, and accountability in data handling. While its success will depend on effective implementation, the Act sets a clear path for businesses and public bodies to build trust with users and handle data responsibly.

As India continues its journey as a digital powerhouse, the DPDP Act ensures that privacy is not left behind in the march of progress.