The Digital Personal Data Protection Bill, 2022

The **Digital Personal Data Protection Bill, 2022** (DPDP Bill) is an important piece of proposed legislation in India designed to establish a framework for the protection of personal data. It is aimed at balancing the need for privacy and data protection with the requirement for economic growth and innovation. Below is a detailed overview of the bill, its components, and its implications.

---

1. PRELIMINARY

Objective

The DPDP Bill aims to safeguard the digital personal data of individuals (referred to as "Data Principals") while regulating how organizations (referred to as "Data Fiduciaries") process such data. It ensures:

- Accountability of entities handling personal data.
- Empowerment of individuals with rights over their data.
- Establishment of a robust regulatory framework.

Key Definitions

- **Data Principal**: The individual to whom the personal data pertains.
- **Data Fiduciary**: An entity (individual, company, or government) that determines the purpose and means of processing personal data.
- **Processing**: Any operation performed on personal data, such as collection, storage, usage, or disclosure.
- **Personal Data**: Any data about an individual that can identify them.
- **Consent**: Freely given, specific, informed, and unambiguous indication of the Data Principal's agreement to process their personal data.

Scope

The bill applies to:

- Processing of digital personal data within India.
- Processing outside India if it involves offering goods/services to individuals in India or monitoring their behavior.

---

2. OBLIGATIONS OF DATA FIDUCIARY

Data Fiduciaries have several obligations to ensure the lawful and transparent processing of personal data.

1. Lawful Processing

Processing must be done for a lawful purpose, with the consent of the Data Principal or under specific exemptions provided by the bill (e.g., legal or governmental requirements).

2. Consent Management

- Consent must be obtained before processing personal data.
- It must be clear, specific, and easily withdrawable.
- Fiduciaries must provide mechanisms for Data Principals to manage and withdraw their consent.

3. Purpose Limitation

Data Fiduciaries can process personal data only for the purposes specified at the time of obtaining consent.

4. Data Minimization

Only data necessary for the specified purpose can be collected and processed.

5. Storage Limitation

Personal data should not be retained longer than necessary for its intended purpose.

6. Accountability

- Fiduciaries must ensure compliance with the provisions of the bill.
- They must implement security safeguards to prevent data breaches.

7. Appointment of Data Protection Officer (DPO)

Significant Data Fiduciaries (large-scale processors of sensitive data) must appoint a DPO responsible for compliance and grievance redressal.

---

3. RIGHTS & DUTIES OF DATA PRINCIPAL

The bill empowers individuals with several rights to control their personal data.

Rights of Data Principals

1. **Right to Access**
   Individuals can request details about the processing of their data and obtain copies of their data.
2. **Right to Correction**
   Data Principals can request corrections or updates to their data.
3. **Right to Erasure**
   They can request the deletion of their data when it is no longer necessary or consent is withdrawn.
4. **Right to Portability**
   Data Principals can transfer their data from one fiduciary to another in a structured format.
5. **Right to Grievance Redressal**
   Individuals can file complaints with the Data Fiduciary or the proposed Data Protection Board if their rights are violated.

Duties of Data Principals

1. **Providing Accurate Information**
   Data Principals must provide accurate and updated information to Fiduciaries.
2. **Compliance with the Law**
   Individuals must avoid filing frivolous or false grievances.

---

4. SPECIAL PROVISIONS

The DPDP Bill contains specific provisions for unique contexts:

1. Processing for Public Interest

Personal data may be processed without consent for:

- Prevention and investigation of crimes.
- Disaster management.
- Public health emergencies.

2. Data of Children

- Parental consent is mandatory for processing data of individuals below 18 years.
- Fiduciaries must not engage in activities harmful to children.

3. Cross-Border Data Transfers

The government may notify specific countries or territories where data can be transferred. This ensures data security and compliance with international standards.

4. Significant Data Fiduciaries

Organizations handling large volumes of sensitive personal data are designated as "Significant Data Fiduciaries" and are subject to additional obligations, such as regular audits and risk assessments.

---

5. COMPLIANCE FRAMEWORK

The DPDP Bill introduces a comprehensive compliance framework for entities handling personal data.

1. Data Protection Board

The **Data Protection Board of India** will be established to:

- Monitor compliance with the bill.
- Address grievances and disputes.
- Impose penalties for violations.

2. Penalties

- Non-compliance with data protection obligations can result in financial penalties, ranging up to ₹500 crore for severe breaches.
- Lesser penalties are imposed for issues like inadequate grievance redressal mechanisms.

3. Audits and Assessments

- Significant Data Fiduciaries must conduct regular data protection impact assessments and audits.
- They must maintain records of processing activities for transparency.

4. Grievance Mechanisms

- Fiduciaries must establish systems for addressing complaints from Data Principals.
- Appeals can be escalated to the Data Protection Board if unresolved.
