DIGITAL PERSONAL DATA PROTECTION BILL, 2023

MINISTRY OF LAW AND JUSTICE

The Digital Personal Data Protection Act 2023, has been enacted by the Parliament to provide for the processing of digital personal data in a manner that recognizes both the right of Individuals, to protect their data and the need to process such personal data for lawful purposes and matters connected therewith or incidental thereto. The provision of the Act shall apply within the territory of India and also outside of the Indian territory if such processing is connected with any activity related to goods or services within the territory of India. This Act shall not apply to personal data processed by an individual for any personal or domestic purpose and is made or caused to be made publicly available.

HIGHLIGHT OF THE BILL:

- The Digital Data Protection Bill 2023, aims to regulate the collection, storage, processing, and sharing of personal and sensitive data in the digital sphere.
- The bill introduces stringent data breach notification requirements, mandating organizations to report data breaches to authorities and affected individuals within a specific timeframe.
- It establishes the concept of a Data Protection Officer (DPO) within the organizations. DPOs act as intermediaries between the organization and the Data Protection Authority for handling data protection issues and inquiries.
- The bill includes provisions for the cross-border transfer of data, outlining conditions under which data can be transferred to other countries or entities.
- The bill imposes fines and penalties for non-compliance with data protection regulations, with the severity of penalties often tied to the nature and scale of the violation.
- The bill also addresses issues related to children's data protection, requiring special safeguards and parental consent for processing the data of minors.

The Bill seeks to provide for the protection of personal data and the privacy of individuals.

- **INTRODUCTION AND SCOPE:**

  The bill begins with an introduction highlighting the importance of protecting personal data in the digital age. It defines key terms and establishes the scope of the legislation, which applies to data controllers and processors operating within the jurisdiction. It emphasizes the need for individuals to have control over their data and sets the stage for the subsequent provisions.

- **DATA PROTECTION AUTHORITY:**

  The bill establishes a Data Protection Authority (DPA) as an independent regulatory body responsible for enforcing the provisions of the legislation. The DPA is granted powers to monitor, investigate, and take action against violations of data protection rules. It also promotes awareness and education regarding data protection.

- **DATA PROTECTION PRINCIPLES:**

  The bill outlines a set of principles that data controllers and processors must adhere to when collecting, processing, or storing personal data. These principles include transparency, purpose limitation, data minimization, accuracy, storage limitation, and accountability. Entities handling personal data are required to follow these principles to ensure fair and lawful data processing.

- **ACCOUNTABILITY:**

  To ensure accountability, the bill mandates that data controllers implement appropriate security measures to protect personal data from breaches and unauthorized access. In the event of a data breach, both data controllers and processors are required to notify the appropriate authorities and affected data subjects within a specified timeframe.

- **INDIVIDUALS RIGHTS:**

  The legislation grants individuals a range of rights concerning their data. These rights include the right to access their data, correct inaccuracies, withdraw consent and erase personal data under certain circumstances. Individuals also have the right to data portability, allowing them to transfer their data between service providers.

- **DATA FIDUCIARY:**

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

  OBLIGATION OF DATA FIDUCIARY:

  1. To make reasonable efforts to ensure the accuracy and completeness of data.
  2. Implement appropriate measures to protect Personal Data in its possession or under its control.
  3. Respond to any communication from the Data Principal for the exercise of her rights.
  4. Inform the Data Protection Board of India and affected persons in the event of personal breach, and
  5. Erase Personal Data as soon as the purpose has been met and retention is not necessary for legal purposes.

- **CONSENT AND PROCESSING:**

  The bill places a strong emphasis on obtaining informed and explicit consent from individuals before processing their data. Consent must be freely given, specific, informed, and capable of being withdrawn. The bill provides guidelines for obtaining valid consent and highlights instances where processing personal data without consent is permissible.

- **SENSITIVE PERSONAL DATA AND CRITICAL DATA:**

  For recognizing the sensitivity of personal data, like health, financial, sexual orientation, religious belief, etc. The bill introduces the concept of "sensitive personal data" and "critical data" and special safeguards are put in place for the processing of these types of data, including health records, biometric information, and data related to national security.

- **CROSS-BORDER DATA TRANSFERS:**

  The bill addresses the cross-border transfer of personal data by requiring data controllers and processors to ensure that such transfers comply with data protection standards. Transfer of personal data to countries lacking adequate data protection standards is subject to specific safeguards, such as the use of standard contractual clauses or binding corporate rules.

- **GOVERNMENT ACCESS TO DATA:**

  The bill addresses government access to personal data for security and law enforcement purposes and for this, specific procedures and safeguards are established by the government to ensure accountability and transparency of data.

- **CHILDREN'S DATA PROTECTION**

  The bill contains provisions for special protection of children's data, with stricter rules for processing and safeguards for minors.

- **DATA PROTECTION IMPACT ASSESSMENT:**

  Data Protection Impact Assessments (DPIAs) assessments evaluate the potential impact of data processing on individuals' privacy and help to identify and mitigate risks. The entities engaged in high-risk processing activities are required to conduct Data Protection Impact Assessments (DPIAs).

- **DATA BREACH NOTIFICATION:**

  The bill mandates the reporting of data breaches to the DPA and affected individuals. Data controllers and processors are required to take prompt action to mitigate the impact of breaches and prevent further unauthorized access.

- **PENALTIES AND ENFORCEMENT:**

  To ensure compliance, the bill outlines a range of penalties for violations, including fines and sanctions. Serious breaches can result in substantial financial penalties. The DPA has the authority to conduct investigations, audits, and inspections to monitor compliance.

- **PRIVACY BY DESIGN AND ACCOUNTABILITY:**

  The legislation promotes the concept of "privacy by design", requiring data protection measures to be integrated into the development of products and services. Data controllers and processors are expected to implement appropriate technical and organizational measures to safeguard personal data.

- **EXCEPTION AND EXEMPTION:**

  This bill outlines specific circumstances where certain provisions may not apply, such as for journalistic purposes, research, and other legitimate interests. The central government may, by notification, exempt certain activities from the application of the Bill. These include: (i) processing by government entities in the interest of the security of the state and public order, and (ii) research, archiving, or statistical purposes. However, these exceptions are subject to balancing individual rights and public interests.