The Digital Personal Data Protection Act, 2023

Highlights of the Bill

The Bill will apply to the processing of digital personal data within India where such data is collected online, or collected offline and is digitized. It will also apply to such processing outside India, if it is for offering goods or services in India.

Personal data may be processed only for a lawful purpose upon consent of an individual. Consent may not be required for specified legitimate uses such as voluntary sharing of data by the individual or processing by the State for permits, licenses, benefits, and services.

Data fiduciaries will be obligated to maintain the accuracy of data, keep data secure, and delete data once its purpose has been met.

The Bill grants certain rights to individuals including the right to obtain information, seek correction and erasure, and grievance redressal-.

The central government may exempt government agencies from the application of provisions of the Bill in the interest of specified grounds such as security of the state, public order, and prevention of offences.

The central government will establish the Data Protection Board of India to adjudicate on non-compliance with the provisions of the Bill.

Key Features of Bill

Applicability

The Bill applies to the processing of digital personal data within India where such data is: (i) collected online, or (ii) collected offline and is digitised. It will also apply to the processing of personal data outside India if it is for offering goods or services in India. Personal data is defined as any data about an individual who is identifiable by or in relation to such data. Processing has been defined as wholly or partially automated operation or set of operations performed on digital personal data. It includes collection, storage, use, and sharing.

Consent

Personal data may be processed only for a lawful purpose after obtaining the consent of the individual. A notice must be given before seeking consent. The notice should contain details about the personal data to be collected and the purpose of processing. Consent may be withdrawn at any point in time. Consent will not be required for 'legitimate uses' including: (i) specified purpose for which data has been provided by an individual voluntarily, (ii) provision of benefit or service by the government, (iii) medical emergency, and (iv) employment. For individuals below 18 years of age, consent will be provided by the parent or the legal guardian.

Rights and duties of data principal

An individual whose data is being processed (data principal), will have the right to: (i) obtain information about processing, (ii) seek correction and erasure of personal data, (iii) nominate another person to exercise rights in the event of death or incapacity, and (iv) grievance redressal. Data principals will have certain duties. They must not: (i) register a false or frivolous complaint, and (ii) furnish any false particulars or impersonate another person in specified cases. Violation of duties will be punishable with a penalty of up to Rs 10,000.

Obligations of data fiduciaries

The entity determining the purpose and means of processing, (data fiduciary), must: (i) make reasonable efforts to ensure the accuracy and completeness of data, (ii) build reasonable security safeguards to prevent a data breach, (iii) inform the Data Protection Board of India and affected persons in the event of a breach, and (iv) erase personal data as soon as the purpose has been met and retention is not necessary for legal purposes (storage limitation). In case of government entities, storage limitation and the right of the data principal to erasure will not apply.

Transfer of personal data outside India

The Bill allows transfer of personal data outside India, except to countries restricted by the central government through notification.

Exemptions

Rights of the data principal and obligations of data fiduciaries (except data security) will not apply in specified cases. These include: (i) prevention and investigation of offences, and (ii) enforcement of legal rights or claims. 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.

Data Protection Board of India

The central government will establish the Data Protection Board of India. Key functions of the Board include: (i) monitoring compliance and imposing penalties, (ii) directing data fiduciaries to take necessary measures in the event of a data breach, and (iii) hearing grievances made by affected persons. Board members will be appointed for two years and will be eligible for re-appointment. The central government will prescribe details such as the number of members of the Board and the selection process. Appeals against the decisions of the Board will lie with TDSAT.

Penalties

The schedule to the Bill specifies penalties for various offences such as up to: (i) Rs 200 crore for non-fulfilment of obligations for children, and (ii) Rs 250 crore for failure to take security measures to prevent data breaches. Penalties will be imposed by the Board after conducting an inquiry.

Way forward

For 3i Infotech to build data privacy within an organization

Assess the current state and start building data privacy within the organisation :- It begins with an evaluation of the existing level of adherence to the Data Protection and Privacy Act (DPPA). A privacy structure should be established, including a Data Protection Officer (DPO) and representatives from different departments. Key applications/databases that store/process personal data should be identified, as well as any downstream applications. Third parties such as service providers must be identified, and agreements/contracts must be amended to ensure their obligations are met.

Take first-level measures to establish mechanisms: - Prepare approved updated versions of documents like data privacy policy, define standard contractual clauses, determine consent types, design consent mechanisms, implement mechanisms requiring individual's clear affirmative action for consent, establish processes for data principal rights, prepare procedures for request acceptance, validation and response, and establish processes for data privacy breach management.

Take next level measures to ensure data protection:- Categorize different types of data and determine the minimum retention period based on inventory gathered. Leverage privacy technology solutions to automate data principal rights, conduct data protection impact assessments, evaluate measures provided, assess compatibility and scalability with existing IT infrastructure. Develop communications and awareness plans, provide training/awareness sessions to stakeholders, and refer to recent notifications/amendments from Central Govt.

Thank You

Legal & Compliance Team 3i Infotech