A LAW MIRED IN SECRECY AND CONTROVERSY!

The journey towards a data protection legislation can be traced back to 2017 when an expert committee was constituted by the Ministry of Electronics and Information Technology (MeiTY).

The major development came in December 2021 when the draft of **Data Protection Bill, 2021 (DPB, 2021) was released.**

However, it was withdrawn in Parliament by Minister for Communications and Information Technology Ashwini Vaishnaw on August 3, 2022.

- ✓ On November 18, 2022, a new draft of the Digital Personal Data Protection Bill, 2022 (DPDPB, 2022) was released for public consultation.
- ✓ The submissions made under this consultation process were not made public.
- ✓ The request to publicly release the submissions was also denied a Right to Information application.
- ✓ One year on, the 2023 Bill has been tabled in Parliament with clarifying how and on what basis these changes were incorporated.

THE PRIMARY OBJECTIVE OF THE DIGITAL PERSONAL DATA PROTECTION BILL, 2023

Is to establish a comprehensive framework for the protection of personal data.

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 operations or set of operations performed on digital personal data. It includes collection, storage, use and sharing.

KEY FEATURES OF THE BILL

Applicability

The Bill applies to the processing of digital personal data within India where such data is:

(i) collected online
(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.

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Consent may be withdrawn at any point in time.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
(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 (individual)

An individual whose data is being processed (data principal), will have the right to:

- ✓ obtain information about processing
- ✓ seek correction and erasure of personal data
- ✓ nominate another person to exercise rights in the event o death or incapacity
- ✓ grievance redressal

Data principals will have certain duties

They must not:

- ✓ Register a false or frivolous complaint.
- ✓ Furnish any false particulars or impersonate another person in specified cases.
- ✓ Violation of duties will be punishable with a penalty of up to I 10,000.

Obligations of data fiduciaries

The entity determining the purpose and means of processing, (data fiduciary), must:

- ✓ make reasonable efforts to ensure the accuracy and completeness of data, build reasonable security safeguards to prevent a data breach
- ✓ inform the Data Protection Board of India and affected person in an event of a breach.

Obligations of data fiduciaries

- ✓ 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 though notification.

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

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
(iii) hearing grievances made by affected persons.

The DPB has the authority to

- ✓ inspect documents of companies handling personal data
- ✓ summon and examine individuals under oath
- ✓ recommend blocking access to intermediaries that repeatedly breach the bill's provisions.

Tenure of Board

- ✓ 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 (Telecom Disputes Settlement and Appellate Tribunal)

Penalties will be imposed by the Board after conducting an inquiry.

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
(ii) Rs 250 crore for failure to take security measures to prevent data breaches.

WHO DOES IT EXEMPT?

Bill exempts government authorities

According to the Bill, the central government will have the right to exempt "any instrumentality of the state" from adverse consequences citing

- ✓ national security
- ✓ relations with foreign governments
- ✓ maintenance of public order, among other things.

IT Minister Ashwini Vaishnaw said that exemptions to the Centre were needed.

"If there is a natural disaster like an earthquake, will the government have time to seek consent for processing their data or have to act quickly to ensure their safety?"

If the police are conducting an investigation to catch an offender, should their consent be taken.

Personal data which is processed for research, archiving, or statistical purposes will also be exempted under this Bill.

NEED FOR THIS BILL?

- ✓ Data breaches are becoming regular occurrences.
- ✓ It was reported in June 2023 that a major privacy breach with respect to the CoWIN portal had taken place.
- ✓ Personal details of vaccinated users had been leaked on Telegram.

Recently, in July 2023, about 12,000 confidential records of State Bank of India employees were reportedly made public on Telegram.

In view of this, a cause of great concern that arises in the Bill is the exemption under Clause 17(2)(a) which, if notified, is granted to the government and its authorities.

CONCERNS

- ✓ Exemptions to data processing by the State on grounds such as national security may lead to data collection, processing, and retention beyond what is necessary. This may violate the fundamental right to privacy.
- ✓ The Bill does not grant the right to be forgotten to the data principal.
- ✓ The Bill allows transfer of personal data outside India, except to countries notified by the central government.

This mechanism may not ensure adequate evaluation of data protection standards in the countries where transfer of personal data is allowed.

CRITICISM

- ✓ Clause 44(3) of the bill seeks to amend the entire Section 8(1)(j) of the Right to Information (RTI) Act, 2005
- ✓ And replace it with "***information which relates to personal information***", has received heavy criticism from stakeholders.

The RTI Act currently allows public authorities to disclose personal information, such as officials' salaries, when it is in the public interest.

The Bill would remove these caveats and completely disallow disclosing personal information.

Exclude the application of Section 43A

Section 43A of the Information Technology Act, 2000 (IT Act) imposes an obligation on corporates to award damages to affected persons in case of negligent handling of their sensitive data.

Clause 44(2) of the Bill aims to exclude the application of Section 43A, thereby rendering an individual who has suffered breach of their data without any relief.

KEY FINDINGS

In studying the Digital Personal Data Protection Act 2023 (DPDPA), several key findings are evident:

Comprehensive Data Protection: The DPDPA provides a comprehensive framework for the protection of personal data, emphasizing the importance of individuals' privacy rights.

Data Subject Rights: The act grants individuals' greater control over their personal data, including the right to access, rectify, and delete their information.

Data Processor Responsibility: The DPDPA places significant responsibilities on data processors to ensure the secure processing of data.

Data Breach Notification: It mandates the reporting of data breaches to both the regulatory authority and affected individuals, promoting transparency and swift action in case of security incidents.

TECHNICAL DETAILS

DPDPA Act: Technical Details:

The DPDPA, being a crucial piece of legislation, contains several technical details that organizations, including UPES, must pay attention to:

Data Minimization and Purpose Limitation: Organizations must collect only the data necessary for the intended purpose and cannot process personal data beyond what is required.

Security Measures: Data controllers and processors must implement appropriate security measures to protect personal data from unauthorized access, disclosure, alteration, and destruction.

Data Protection Impact Assessments (DPIAs): Conduct DPIAs for high-risk data processing activities to identify and mitigate privacy risks.

Cross-Border Data Transfers: Ensure that international data transfers comply with the act's requirements, including the use of standard contractual clauses or other approved mechanisms.

Consent Management: Establish mechanisms for obtaining clear and informed consent from data subjects and enable them to withdraw consent easily.

CASE STUDIES

Case Study 1: Student Records Protection

Background:

UPES collects and processes personal data of students, including academic records, contact information, and financial data.

DPDPA Compliance:

The university must ensure that it collects only necessary data, obtains informed consent, and implements robust security measures to protect student records. Additionally, UPES should develop a clear procedure for students to access and rectify their data.

Case Study 2: Research Data Handling

Background:

UPES conducts research involving personal data collected from research participants.

DPDPA Compliance:

Researchers at UPES must perform DPIAs for research projects involving personal data, ensuring that privacy risks are addressed. Consent from research participants should be explicit, and data should be anonymized whenever possible to minimize data processing.

Case Study 3: Employee Data Security

Background:

UPES manages personal data of its employees, including payroll information and HR records.

DPDPA Compliance:

The university should review its data security measures for employee data, ensuring that access is restricted to authorized personnel. Clear guidelines for data access, retention, and disposal should be established in line with the DPDPA.

CONCLUSION

The Digital Personal Data Protection Act 2023 imposes critical obligations on organizations like UPES to protect personal data and respect individuals' privacy rights. As the Chief IT Security Officer, it is imperative to proactively assess and adapt UPES's data handling and security practices to ensure compliance with the act, as outlined in the technical details and case studies provided above.

This report serves as a starting point for UPES's journey towards full compliance with the DPDPA and enhancing cyber awareness within the organization. It is recommended that UPES establish a cross-functional team to oversee compliance efforts and conduct regular audits to ensure ongoing adherence to the act's provisions.