Information Technology Laws
Vol. 3: No. 38
December 26, 2022

Malavika Ramanand
Associate

DIGITAL PERSONAL DATA PROTECTION BILL – AN ANALYSIS
PART I

A. Introduction

On November 18, 2022, the Union Ministry of Electronics and Information Technology (**MeitY**) withdrew the Personal Data Protection Bill, 2019 (**PDP Bill**), and released the Digital Personal Data Protection Bill, 2022 (**the Bill**)[1] for public consultation.[2] Once passed by the Parliament and notified, the Act is expected to be implemented in phases. The Bill seeks to establish a comprehensive framework of protection of digital personal data; detailing rights and duties of Data Principals and restructuring the compliance obligations of Data Fiduciaries.

The 'Explanatory Note' to the Bill explains that the proposed law is based on seven principles of the 'data economy', including data minimisation, accuracy and limited retention, implementation of safeguards and accountability for processors.[3]

This part summarises chapters I-II of the Bill, and Part II will yield focus to chapters III-VI.

B. Key Features

1. Definitions

a. "**Data Principal**" is defined broadly and refers to the "*individual to whom the data relates*", and in the context of a child (under 18 years of age), the parent or lawful guardian of that child.[4] "**Data Fiduciary**" refers to any person who (alone or in conjunction with others) determines the purpose and means of processing personal data.[5]

b. "**Harm**" is limited to actual bodily harm, distortion or theft of identity, harassment, or prevention of lawful gain or causation of significant loss, in relation to a Data Principal.[6] "**Loss**" and "**Gain**" refer to narrowly defined financial losses and gains.

This contrasts with the expansive definition of "harm" as per the PDP Bill, which also included *inter alia* reputation/employment loss, discrimination, denial of service or benefit resulting from a decision of Data Principal, and restrictions on speech/movement, or actions arising out of fear of surveillance.[7] This limited definition of "harm" could potentially lead to lesser accountability on part of Data Fiduciaries, especially when penalties for non-compliance under the Bill is not computed based on extent of harm suffered by a Data Principal.

---

[1] The Bill is accessible here.
[2] Response timeline extended to Jan 2, 2023.
[3] The Explanatory Note is accessible here.
[4] Clause 2(6) of the Bill.
[5] Clause 2(5) of the Bill.
[6] Clause 2(10) of the Bill.
[7] Clause 2(20), PDP Bill, accessible here.

c. "**Personal Data**" is defined as "*any data about an individual who is identifiable by or in relation to such data.*"[8] This may potentially mean that "non-identifiable data" may not qualify under this definition.

   This contrasts with the definition in the PDP Bill, where protections were afforded to non-identifiable data, which in combination with other data could result in personally identifiable information. Critically, the Bill departs from the current legal regime,[9] where additional protection is afforded to "sensitive personal data or information".[10] The Bill does not differentiate between personal data and sensitive/critical personal data, and thus the protections under it appear to be common for all categories of personal data.

d. "**Personal Data Breach**" is defined as "*any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.*"[11]

e. "**Public Interest**" is defined expansively in the Bill and encompasses state sovereignty, security, friendly relations with foreign states, maintenance of public order, preventing incitement of commission of cognizable offences, and preventing dissemination of false information. The Bill introduces the concept of "deemed consent" where consent is deemed to have been given, if the requirement for processing is in public interest.

2. Notice

a. The Bill requires Data Fiduciaries to provide Data Principals with a notice, before obtaining their consent for processing of personal data. It must be presented in clear and accessible language and contain information on the personal data that is collected and the purpose of processing.
b. Data Principals must also be given an option to access the notice in English, or any other official language.[12]

3. Express Consent

a. Consent under the Bill means any freely given, specific, informed, and unambiguous indication of Data Principal, by which they signify their agreement to the processing of personal data. The request for consent must be presented in clear and plain language, in English or any other official language.[13]
b. Data Principals must be given the option to review, manage, or withdraw their consent.
c. Data Fiduciary must, within a "reasonable timeframe" cease the processing of such data if consent is revoked, unless the consent is required or authorised under the Bill or any other legal provision.
d. The Bill introduces "**Consent Managers**" who act as Data Fiduciaries, and enable Data Principals to give, manage, review, and rescind consent through accessible and transparent means. Consent Managers must be registered with Data Protection Board established by the Central Government.

4. Deemed Consent

a. This is introduced where Data Principal is deemed to have given consent to the processing of personal data if it is "necessary" in specified scenarios such as:[14]

---

[8] Clause 2(13) of the Bill.
[9] Information Technology (Reasonable Security Practices and procedures and Sensitive Personal Data or Information) Rules, 2011 (**IT Rules**) under the Information Technology Act, 2000.
[10] Rule 3, IT Rules.
[11] Clause 2(14) of the Bill.
[12] As specified in the Eighth Schedule of the Constitution of India.
[13] ibid.

i. Personal information is voluntarily provided by Data Principal, *e.g.*, giving name and number to restaurant for reservations;
ii. Performing any function under law or the State's providing any service or benefit to Data Principal;
iii. Compliance with any judgment or order issued under law;
iv. Availing health services;
v. Providing services during any disaster, or breakdown of public order;
vi. For employment purposes, prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, *etc.*;
vii. Public interest, *e.g.*, prevention and detection of fraud in corporate restructuring, operating search engines to process publicly available personal data, network and information security, debt recovery; or
viii. Other fair and reasonable purposes where interests of Data Fiduciary outweigh the adverse effect on rights of a Data Principal, any public interest considerations, and reasonable expectations of Data Principal.

b. It appears from this novel introduction that notice need not be served on Data Principals in cases where consent is deemed. Data Fiduciaries must simply establish that the processing of personal data was reasonably expected, or it fell under the above scenarios.

---

[14] Clause 8 of the Bill.