PARINAM
LAW ASSOCIATES

OVERVIEW OF THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

I. INTRODUCTION:

The Ministry of Electronics and Information Technology ("**MEITY**") on 18 November 2022 has released the Digital Personal Data Protection Bill, 2022 ("**Bill**") with a view to regulate the processing of digital personal data within India, as well as outside India in the case of profiling and/or targeting of Indian users accessing such data. The Bill marks a watershed moment in India's legislative history as it protects citizens' privacy against not only Indian corporations, but also major multinational companies.

II. KEY HIGHLIGHTS:

As per the Bill released on the website of the MEITY, the key highlights are as follows:

- **Important Terms Used:**

  The Bill defines data fiduciary, data principal, and data processor.

  - Broadly, data fiduciary means a person or persons who determine the purpose and means of processing personal data.
  - Data principal means the person whose personal data is being processed.
  - Data processor means a person who processes such personal data on behalf of the data fiduciary.
  - Apart from these terms, the Bill also contemplates the classification of certain data fiduciaries as significant data fiduciaries by the Central Government based on various relevant factors such as the volume and sensitivity of personal data processed; risk of harm to the data principal; potential impact on the sovereignty and integrity of India; public order; etc. Such significant data fiduciaries are tasked with the appointment of data protection officers as well as independent data auditors and the conduct of data protection impact assessments and periodic audits.

- **Extra-Territorial Application:** The scope of the Bill is extra-territorial in nature, as seen in Section 4, whereby it is stated that the Bill applies to the processing of digital personal data within the territory of India, as well as to the processing of digital personal data outside the territory of India, if it is in

connection with any profiling activity or activity relating to offering of goods and services to data principals situated within the territory of India. Profiling has been further explained as a form of processing personal data which either analyses or predicts aspects related to the behaviour, attributes, or interests of a data principal. This provision has important ramifications for big-tech companies located outside India, which routinely process the personal data of Indian citizens, particularly for the purpose of targeted advertisements. The Central Government has also been given the authority to designate countries or territories outside India where a data fiduciary may transfer personal data if necessary.

- **Conditions & Manner of Processing Personal Data:** Notably, the Bill lays down twofold criteria for the processing of digital personal data of a data principal, which is (i) the processing must be for a lawful purpose, and (ii) the data principal must have given or been deemed to give their consent for such processing. A data fiduciary is obligated to provide the data principal with an itemised notice containing a description of the personal data sought to be procured and the purpose for doing so, along with an option to the data principal to access the said notice either in English or any language specified in the Eight Schedule to the Constitution of India. The notice must also contain the contact details of the relevant data protection officer. Data principals have been given the right to obtain confirmations with respect to the processing of personal data by a data fiduciary, as well as a summary of the personal data processed or under process by the data fiduciary along with the identities of those entities with whom such personal data has been further shared. Data principals may also correct or erase personal data collected by a data fiduciary by putting forth a request in the prescribed form. The concomitant duties of a data principal include compliance with the provisions of the Bill, registering of genuine and non-frivolous complaints, providing of genuine information and refraining from identity fraud or theft.

- **Consent of a Data Principal:** The criterion of consent has been made revocable at the instance of the data principal, provided that the personal data which has already been processed before the withdrawal of consent will be lawful and pursuant to the withdrawal of consent, the relevant data fiduciary must itself cease and also cause its data processors to cease the further processing of such data. The burden of proof with respect to the giving of consent by a data principal is on the data fiduciary, who must prove that due notice was given by it. Data fiduciaries must ensure that they cease to retain personal data or the means of accessing it as soon as the purpose for which it was collected is no longer being served and its retention is no longer necessary for legal or business purposes. Additionally, the giving, managing, and reviewing of a data principal's consent must be done through a consent manager, who is an entity

accountable to and acting on behalf of the data principal and registered with the Data Protection Board of India ("**Board**") established by the Central Government.

- **Deemed Consent:** While consent of the data principal as contemplated under the Bill is an important means of preventing misuse of personal data, the Bill in Section 8 also provides for the concept of deemed consent in various scenarios, as outlined below:

    - To begin with, deemed consent can be read into a situation where the data principal voluntarily provides their personal data to a data fiduciary, and it is reasonably expected that they would do so. For example, while making a dinner table reservation at a restaurant, it is reasonably expected that the data principal would provide such restaurant with her name and mobile number, and the restaurant may use such information towards the facilitation of the reservation, such as calling the provided number to confirm the reservation.

    - Deemed consent would also apply in a scenario where the State or any of its instrumentalities must perform a function as per law or for the provision of any service or benefit to the data principal, such as the grant of certificates, licenses, or permits using the personal data of the data principal.

    - Where personal data is required to be processed in compliance with any judgment or order issued under any law, the data principal will be deemed to have provided consent for such processing.

    - In cases where there is a medical emergency posing an immediate threat to the life or health of the data principal or any other individual, the processing of personal data will be deemed to have been obtained with the consent of the data principal. This may be extended to situations wherein measures have to be taken to provide medical treatment to individuals during epidemics or other instances which involve threats to public health.

    - Consent may be deemed to have been given in cases involving breakdown of public order or disasters, where it becomes necessary to process personal data to ensure the safety of individuals.

    - Personal data may also be used with deemed consent for the purposes of employment, such as in scenarios where the data principal being an employee of a company provides the said company with her biometric data, and such company uses the biometric data to record her attendance.

- Lastly, deemed consent would be applicable in public interest such as prevention and detection of fraud, corporate restructuring transactions under applicable laws, network and information security, processing of publicly available personal data, and recovery of debt.

- Importantly, deemed consent for processing of personal data must be balanced with any overarching adverse effects on the rights of the data principal, and any public interest, and the reasonable expectations that a data principal would have with respect to the context of the processing.

- **Breach of Personal Data:** An extremely important aspect of the Bill is the treatment of personal data breach, which has been explained under Section 9, along with the general obligations of a data fiduciary. The Bill mandates that a data fiduciary must notify the Board as well as the affected data principal in the event of a personal data breach. The failure of a data processor or data fiduciary to take reasonable measures to avoid an event of personal data breach would result in a penalty of up to rupees two hundred and fifty crore, and any failure to notify the Board and affected data principals after the occurrence of a breach of personal data would result in a penalty of rupees two hundred crore. Thus, we observe that the Bill has endeavoured to provide a robust mechanism for the protection of individual privacy.

- **Grievance Redressal Mechanisms:** The Board has vide Section 21 sub-clause (13) been given authority equivalent to that of a Civil Court as provided for under the Code of Civil Procedure, 1908. Upon receipt of a complaint or reference, the Board may authorise the initiation of proceedings while first determining if there exist sufficient grounds to initiate an inquiry. Upon conclusion of such inquiry, the Board may impose financial penalties up to rupees five hundred crore. Further, the Board has been given the power to review its own orders and appeals against orders of the Board may be made to the relevant High Court. The jurisdiction of other civil courts has been explicitly barred. Provision has been made to authorise the Board to direct disputes to mediation or other dispute resolution forms. Lastly, the Board may accept voluntary undertakings related to any compliance measures mentioned in the Bill. Providing such a voluntary undertaking would have the effect of a bar on proceedings mentioned hereinabove.

III. CONCLUSION:

The Bill is a doubtlessly a necessary piece of legislation considering the recent boom in the digital economy where personal data has become a valuable resource. It has been drafted in consultation with major stakeholders and will be put forth for further

public review before it is enacted. Notably, the transfer of personal data outside India is a feature that was not explicitly carved out in the Personal Data Protection Bill, 2019, which was consequently criticised by major tech companies such as Amazon and Meta. The Bill is also in keeping with global privacy legislations such as the United Kingdom General Data Protection Regulation, 2018. On the other hand, the placing of national and/or public interest over individual interests, particularly in the case of digitally processed personal data could be seen as potential privacy issue. There is also a potential lacuna in the designation of consent managers as those who act on behalf of data fiduciaries and enable data principals to give or withdraw their consent, in as much as, there is no explanation provided for a scenario in which a party may be both a data fiduciary as well as a consent manager.

* * * * *

DISCLAIMER

MUMBAI

4th Floor, Express Towers, Ramnath Goenka Marg, Nariman Point, Mumbai – 400 021

Tel : +91 22 4241 0000

NEW DELHI

4 Todamal Lane, Bengali Market, New Delhi – 110 001

Tel : +91 98104 00283

PUNE

2nd Floor, Kundan Chambers, Thube Park, Next to Sancheti Hospital, Pune – 411 005

Tel : +91 20 2553 0711

WWW.PARINAMLAW.COM