KNOWLEDGE BANK™

Always stay curious

MCO LEGALS

9th December, 2022

CYBER LAW: ISSUE 12

THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022 – HIGHLIGHTS & KEY TAKEAWAYS

Introduction

- On 04.08.2022, the Ministry of Electronics and Information Technology **("MEITY")** announced to withdraw the Data Protection Bill, 2021 which had fought the battle for nearly 5 years to come into action to serve the purpose for which it was introduced, i.e. to protect the personal data of the individuals and guarantee right to privacy of the citizens.
- MEITY then, had promised to come back with a reframed version of the privacy bill.
- Ultimately on 18.11.2022, it published the much awaited draft Digital Personal DataProtection Bill, 2022 **("The Bill")** in the public domain for comments and suggestions.
- The Bill (divided into 6 chapters, 30 clauses, and 1 schedule) focuses only on digital personal data and introduces regulations for the processing of digital personal data in amanner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes.

Highlights -

1. Defining Personal Data – Clause 2(13):

- Defined as 'any data about an individual who is identifiable by or in relation to such data'.
- The definition is framed in lines with European Union's General Data Protection Regulation **("GDPR")**.
- The definition has a broad ambit and has the potential to include various types of data that directly or indirectly identifies a person. However, it doesn't provide any clarity of the level of identification required.
- The Bill has also not considered to further categorise the data into sensitive, or critical and therefore, is not in consciences with the Information Technology Act, 2000 where separate rules are prescribed for sensitive personal data.
- Also, critical personal data such as military or national security data is also not recognised.

2. Scope - Clause 4:

- The Bill shall apply to the processing of digital personal data within the territory of India and outside the territory of India, if such processing is in connection with any profiling of, or activity of offering goods or services to Data Principals within the territory of India.
- The Bill has no applicability on non-automated processing of personal data, offline personal data, personal data processed by an individual for any personal or domestic purpose, and personal data about an individual that is contained in a record that has been in existence for at least 100 years.
- As the Bill has an extra territorial application, it will apply to foreign entities as well as per the provisions of the Bill.

3. Consent and deemed consent - Clause 7:

- The digital personal data processing must be for a lawful purpose with the consent or deemed consent of the Data Principal.
- Consent means any freely given, specific, informed and unambiguous indication of the Data Principal's wishes by which the Data Principal, by a clear affirmative action, signifies agreement to the processing of the personal data for the specified purpose.
- Also, at the time of or before obtaining the consent from the data principal, the Data Fiduciary must give an itemised notice which includes description of personal data sought to be processed and the purpose of processing.
- This implies that while taking the consent, the Data Fidu-

Amit Meharia

Managing Partner, MCO Legals

LLB (Hons) King's College London, Solicitor (Supreme Court of England & Wales)

Expertise:

Corporate Due Diligence & Corporate/Commercial Arbitration

amit.m@mcolegals.co.in

Bhavna Sharma

Research Partner

B.Sc., LLM, Research Scholar, RML National Law University, Lucknow

ciary has to provide only limited information, and no information is needed to be given regarding privacy practices, data transfers, safeguard measures opted by the Data Fiduciary, type of processing and other significant information that a data principle must know especially where sensitive and critical personal data is taken by the Data Fiduciary.

- Some situations where the consent will be a deemed consent –

a. Data Principal voluntarily provides personal data and it is reasonably expected that she would provide such personal data such as for booking in a hotel.

b. processing by state for the performance of any function under law, or provision of any service or benefit to the Data Principal such as for issuance of Voter Id, driving license, etc.

c. compliance with any judgment or order;

d. in case of response to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;

e. providing medical treatment or health services to any individual during epidemic, disease outbreak, or public health crisis like contact tracing;

f. disaster management or public disorder;

g. employment related purposes;

h. in public interest;

i. any other fair and reasonable purpose;

- The concept of deemed consent provided in the Bill is extremely wide in scope and touches almost every situation where the data principal's consent may be considered as a deemed consent especially in case where the government is collecting and processing the personal data of a Data Principal.

- By adding grounds of deemed consent, such as public interest and any other fair and reasonable purpose, creates a situation where the personal data may be used freely in the name of deemed consent.

- In the case of deemed consent, there is no requirement for giving prior notice to the Data Principal, consequently, the Data Principal may not have any information on what, why, how and when their personal data was processed, and this dilutes the transparency and accountability principle which are fundamental for safeguarding informational privacy.

4. <u>General Obligations of Data Fiduciary - Clause 9:</u>

a. It shall make reasonable efforts to ensure that personal data processed is accurate and complete where the use of personal data is likely to affect the Data Principal or is likely to be disclosed by the data fiduciary to another Data Fiduciary.

b. It shall implement appropriate technical and organizational measures to ensure effective adherence with the provisions of the Bill.

c. It shall protect personal data by taking reasonable security safeguards to prevent personal data breach.

d. It shall notify the Data Protection Board in case of data breach.

e. It shall cease to retain personal data or remove the means by which the personal data can be associated with particular data principal, as soon as the purpose for which the personal data was collected is no longer being served by its retention and retention is no longer necessary for legal or business purposes.

f. It shall publish the business contact information of a Data Protection Officer or a person who is able to answer on behalf of data fiduciary, the questions of the data principal about processing of the personal data.

g. Put in place a procedure and effective grievance redressal mechanism.

h. It shall process personal data only under a valid contract.

5. <u>Additional Obligation of Significant Data fiduciary - Clause 11:</u>

- A separate category of Data Fiduciary is recognised which is similar to the concept of significant social media intermediary as opted under the Intermediaries Rules, 2022.

- Under the Bill, the Central Government is empowered to notify any Data Fiduciary as Significant Data Fiduciary based on factors such as volume and sensitivity of personal data processed, risk of harm to data principal, and other factors related to well-being of the state as a whole.

- Some additional obligations are imposed on the Significant Intermediary such as appointing a Data Protection Officer and an Independent Data Auditor and undertake measures such as Data Protection Impact Assessment and periodic audit.

6. <u>Rights and Duties of Data Principal - Chapter 3:</u>

- The Data Principal not only have rights towards its personal data but also have duties in relation to its personal data.

- The rights of the Data Principal are - Right to information, right to correction and erasure of personal data, right of grievance redressal and right to nominate.

- The duties of the Data Principal are – Complying with the laws while exercising rights under this Bill, not to register a fake complaint, not to furnish false information or impersonate others, furnish only such information as it verifiably authentic while exercising the right to correction or erasure. A penalty shall be imposed on the data principal in case of non-compliance with the duties under the Bill.

- The various rights of Data Principals are taken from the GDPR but the rights that have been left to be included without any rational reasonable are – right to be forgotten, right to object certain kind of processing and right to data portability. As Indian Government is coming up with first ever privacy law, it would have included every right of the data principal to justify the whole purpose of the privacy law. Also, how the right will be exercised is also not mentioned in the Bill.

7. <u>Transfer of personal data outside India - Clause 17:</u>

- The Central Government has taken everything over its shoulders while deciding about cross-border data flow.

- After assessing the necessary factors in case of transfer of personal data, the Central Government may notify such countries or territories outside India to which data fiduciary may transfer personal data.
- The Central Government is free to decide terms and conditions for cross border data transfer as it deems fit.
- However, we still need to see if it is in conformity with the present IT Rules on data transfers. The Bill seems to have relaxed the conditions provided under the IT Rules. Also, there is no say on the data localization which was present in the previous version of Privacy Bill, i.e. Data Protection Bill, 2021.

8. Establishment of Data Protection Board of India - Clause 19

- The Bill has established a Data Protection Board of India (**"DPBI"**) which shall consist of chairperson, other members, officers and employees as prescribed by the Central Government.
- The DPBI shall be an independent regulator responsible for the allocation of work, receipt of complaints, formation of groups for hearing, pronouncement of decisions, and other functions as the Central Government may prescribe.
- It shall have all powers to conduct inquiry, summon witnesses, inspect evidence, and impose penalties.
- As privacy is a whole new domain, it was much needed to have separate independent body to deal with the matters related to privacy. It is expected that the composition of the DPBI will be individuals having expertise in the privacy sector to serve the purpose and effective enforcement and implementation of the DPBI framework.

9. Financial Penalties - Clause 25

- The Bill imposes only financial penalties in case of non-compliance which shall not exceed Rs 500 crore in each instance.
- There are various factors that are laid down while determining the amount of financial penalty such as the nature, gravity, duration and repetitive nature of the non-compliance, the type and nature of the personal data affected by the non-compliance; person gained or avoided any loss, mitigation action taken by the person, etc.

Conclusion

- The Bill is short yet comprehensive.
- The Government has followed the minimalistic approach to draft the privacy legislation which is completely justified looking at the nature of technology that keeps on changing every second.
- Putting everything under the one piece and trying to regulate the whole privacy domain may not have been a great idea as the 'one size fit all' approach doesn't work in technology sector.
- Taking the principal based approach and putting the building blocks provisions to address the issues in the privacy sector is how the privacy legislation should be drafted.
- The Bill is open for comments and suggestions; it is expected that the next version of the Bill will definitely provide more clarity to the provisions that lacks explicitness, consider the grey areas which are contradicting the present laws in force and come up with a piece that satisfies all and in an implementable form.