EXPLANATORY NOTE TO DIGITAL PERSONAL DATA PROTECTION BILL, 2022

Introduction

Digital India has caused digitization of the Indian economy and transformed the lives of Indian citizens in particular and governance in general. The lives of crores of Indians and their experience of governance have been significantly enhanced by the use of technology and the internet. Digital India has also unleashed innovation and entrepreneurship in the digital space in addition to the large global Big Tech platforms that have significant presence on the internet.

Presently, there are over 76 crore (760 million) active internet users (Digital Nagriks) and over the next coming years this is expected to touch 120 crore (1.2 billion). India is the largest connected democracy in the world and is amongst the highest consumers and producers of data per capita amongst the countries.

It has become clear over the last few years that while the internet and technology is a force for good and connectivity, it is also a place where user harm and misuse can exist if these rules and laws are not prescribed. That is why laws and rulemaking for the internet has to be around the basic foundational principles and expectations of our citizens of openness, safety & trust and accountability.

Data in general and Personal Data in specific are at the core of this fast-growing Digital Economy and eco-system of digital products, services and intermediation. It has become very clear over the last few years whilst this data is used by platforms and intermediaries, the data and personal data must be subject to a framework of rules and dos and don’ts.

The Digital Personal Data Protection Bill is a legislation that frames out the rights and duties of the citizen (Digital Nagrik) on one hand and the obligations to use collected data lawfully of the Data Fiduciary on the other hand. The bill is based on the following principles around the Data Economy:

The first principle is that usage of personal data by organisations must be done in a manner that is lawful, fair to the individuals concerned and transparent to individuals

The second principle of purpose limitation is that the personal data is used for the purposes for which it was collected.

The third principle of data minimisation is that only those items of personal data required for attaining a specific purpose must be collected.

Disclaimer: The purpose of this explanatory note is only to make it easier to understand the provisions of the Bill. However, this explanatory note is not intended to form part of the Bill and shall not be considered for legal interpretation of any provision of the Bill.

The fourth principle of accuracy of personal data is that reasonable effort is made to ensure that the personal data of the individual is accurate and kept up to date.

The fifth principle of storage limitation is that personal data is not stored perpetually by default. The storage should be limited to such duration as is necessary for the stated purpose for which personal data was collected.

The sixth principle is that reasonable safeguards are taken to ensure that there is no unauthorised collection or processing of personal data. This is intended to prevent personal data breach.

The seventh principle is that the person who decides the purpose and means of processing of personal data should be accountable for such processing.

These principles have been used as the basis for personal data protection laws in various jurisdictions. The actual implementation of such laws has allowed the emergence of a more nuanced understanding of personal data protection wherein individual rights, public interest and ease of doing business especially for startups are balanced.

Consultations

During the drafting of the Personal Data Protection Bill, 2019 the entire gamut of principles was widely debated and discussed. These include rights of individuals, duties of entities processing personal data and regulatory framework among others.

Taking into account these consultations and deliberations, the Government of India has now prepared a draft Digital Personal Data Protection Bill, 2022 ("Bill"). The current draft of the Bill carries forward the understanding that emerged during consultation with stakeholders in the process of drafting the Personal Data Protection Bill, 2019.

The Government considered the global best practices, including review of the personal data protection legislations of Singapore, Australia, European Union and prospective federal legislation of the United States of America. The Government has also considered our 1 trillion-dollar Digital Economy goals and the rapidly growing innovation and startup eco-system.

The Bill will establish the comprehensive legal framework governing digital personal data protection in India. The Bill provides for the processing of digital personal data in

a manner that recognizes the right of individuals to protect their personal data, societal rights and the need to process personal data for lawful purposes.

Drafting practices

Comprehensibility of law for citizens is a desirable goal. Therefore, the Bill has been drafted in a plain and simple language so that even a person with basic understanding of law is able to understand its provisions. The provisions have been concisely and clearly drafted and no provisos have been used. Illustrations and contextual definitions where necessary have been incorporated to further clarify the meaning and intent of provisions.

This explanatory note provides a brief overview of the contents of Bill, to facilitate further consultations.

Chapter-wise Summary of the Bill:

Preamble

1. The purpose of this Bill is to provide for the processing of digital personal data in a manner that recognises the right of individuals to protect their personal data, the need to process personal data for lawful purposes and for other incidental purposes. These incidental purposes include the framework for compliance with provisions of the Bill.

Chapter 1: Preliminary

2. The Bill has been introduced as the Digital Personal Data Protection Bill, 2022.

3. All those terms that have been used in more than one context with a specific intended meaning have been defined in the provision on Definitions.

   The term “Data Principal” has been used to identify the individual to whom personal data is related. Considering the utility and usage of personal data of children, it has been provided that in case of children their parents or lawful guardians of children would be considered Data Principal.

   The definition of “personal data” has been worded in a direct and simple manner to mean any data by which or in relation to which an individual can be identified.

The entity (whether it be an individual, company, firm, state etc) which decides the purpose and means of processing of an individual's personal data has been termed the "Data Fiduciary". The deliberate choice of "Fiduciary" underlines that the relationship between the Data Principal and Data Fiduciary is expected to be one based on mutual trust.

The definition of "processing" has been used to cover the entire cycle of operations that can be carried out in respect of personal data. Thus, several operations right from collection to storage are, as per the definition in the Bill, examples of processing.

In the interest of absolute clarity, "public interest" a phrase often used in law has also been defined.

4. For the first time in India's legislative history, "her" and "she" have been used to refer to individuals irrespective of gender. This is in line with the government's philosophy of empowering women.

Considering the linguistic diversity of India, provision has been made for enabling individuals to access basic information in 8th schedule languages. This would enable individuals to make a fair assessment of a situation where their personal data is being sought and then decide whether they want to share the personal data or not.

6. Internet and digitalisation of data offer great opportunities but also lead to greater challenges. Recognising this and to maintain focus on increasingly digital nature of interactions, the Bill applies to digital personal data.

Chapter 2: Obligations of Data Fiduciary

7. Grounds (in the nature of requirements) on which personal data can be processed have been clearly specified.

First requirement is that personal data of an individual is processed only in accordance with provisions of this Bill.

The second requirement is that such processing is done only for a purpose which is not forbidden by law.

The third requirement is that before the personal data of an individual can be processed, the individual should have either given consent to the processing

for stated purposes or deemed to have given consent in certain limited circumstances.

8. Protection of personal data begins with knowledge about processing. Every individual should know what items of personal data a Data Fiduciary wants to collect and the purpose of such collection and further processing. This is enabled by the provisions related to Notice, in the Bill. It has been stated that the notice from Data Fiduciary to Data Principal should be in a clear and plain language and available in 8th schedule languages.

9. Consent of the individual should, in general, be the basis for processing of her personal data. Detailed provision on Consent has been incorporated in the Bill. Request for consent from Data Fiduciary to Data Principal should be in a clear and plain language and available in 8th schedule languages.

   Consent should not be perpetual and irrevocable in order for individual to exercise meaningful control over her personal data. Thus, it has been provided in the Bill that consent may be withdrawn by the Data Principal.

   The proliferation of Digital Economy has meant that the number of organisations one engages with, has increased exponentially. It is not always possible to keep track of the instances in which one has given consent to processing of personal data. Addressing this issue, an ecosystem of consent managers has emerged. A consent manager platform enables an individual to have a comprehensive view of her interactions with Data Fiduciaries and consent given to them. The Bill has recognised Consent Managers.

10. In several situations, seeking consent of Data Principal is impracticable or inadvisable due to pressing concerns. Clearly defined situations wherein insisting on consent would be counterproductive have been listed under the Deemed Consent provision in the Bill.

11. A Data Fiduciary must be aware of its obligations. Therefore, specific provision listing all obligations of Data Fiduciary has been included in the Bill. The fundamental principle is that a Data Fiduciary is ultimately responsible for processing of personal data of an individual.

    It is the responsibility of Data Fiduciary to ensure that all reasonable safeguards are taken to prevent personal data breach.

    Storage limitation is a widely accepted principle of personal data protection. This has been recognised across the world. In the Bill it has been clearly

provided that a Data Fiduciary must retain personal data only so long as it is required for the purpose for which it was collected.

It is the responsibility of Data Fiduciary to ensure that Data Principal is able to seek effective redressal of his grievances. To facilitate this, it has been provided in the Bill that every Data Fiduciary should publish contact details of the person to whom grievances and queries can be addressed.

12. Personal data of children is a special category on account of the identifiable group i.e. children in need of greater protection. Recognising this, it has been provided in the Bill that no processing of personal data that is likely to cause harm to a child should be done. Further, special role of parents and guardian in the context of children's personal data has been recognised.

13. On account of factors such as volume of personal data, risk of harm to Data Principals etc certain Data Fiduciaries need to be tasked with additional obligations in the interest of Data Principals. Thus, a specific category called Significant Data Fiduciary has been mentioned in the Bill. This category needs to fulfil certain additional obligations to enable greater scrutiny of its practices.

Chapter 3: Rights and Duties of Data Principal

14. Every individual should be able to obtain certain basic information about her personal data. Recognising this, confirmation of processing, summary of personal data, disclosure of identity of Data Fiduciaries with whom personal data has been shared etc have been included within this right to information.

15. From time to time one's personal data may need to be updated e.g. shifting to another city entails change in address. Further, in the process of collecting personal data, few errors may have been made to particulars of personal data. To enable correction, update, completion and also erasure of personal data where it's no longer needed, specific provision in the nature of a right has been included in the Bill.

16. Right to file complaint with Data Fiduciary and right to file grievance with Data Protection Board in case of lack of response or unsatisfactory response has been specified in the Bill.

17. Nomination is a basic practice and right available to individuals in several contexts such as financial services. Learning from this practice, right to nomination in respect of personal data has been specifically included in the Bill.

18. From the perspective of our societal norms as well as our Constitution, duties are as important as rights. Therefore, a specific provision listing basic duties of Data Principals has been included in the Bill. These duties basically aim at ensuring that there is no misuse of rights and exercise of rights does not lead to adverse effect on others' rights.

Chapter 4: Special Provisions

19. Cross-border interactions are a defining characteristic of today's interconnected world. Recognising this, it has been provided in the Bill that personal data may be transferred to certain notified countries and territories. An assessment of relevant factors by Central Government would precede such a notification.

20. Acknowledging national and public interest is at times greater than the interest of an individual, a clear grounds-based description of exemptions has been incorporated in the Bill.

Chapter 5: Compliance Framework

21. The Data Protection Board is the body tasked with enforcement of provisions of this Act. A digital by design compliance framework is the need of the hour particularly when it comes to digital personal data. This has been recognised in the Bill. Receipt of complaints, pronouncement of decision etc has been clearly envisaged as digital by design, in the Bill.

22. Adherence with principles of natural justice at every stage in a proceeding has been clearly mentioned as required in the end-to-end process of inquiry.

23. Voluntary undertaking has been included as a measure to encourage timely admission and rectification of lapses. This would go a long way in establishing clear focus on enabling and facilitating compliance rather than penalising non-compliance.

24. Financial penalty has been prescribed as the deterrent for non-compliance. Criminalisation of lapses and non-compliance has been avoided.

Chapter 6: Miscellaneous

25. Power of Central Government to make Rules, remove difficulties in implementation of the Bill and limited power to amend Schedule have been separately listed.

---

26. The intent is to provide for a general law that applies horizontally across sectors while allowing the scope for sector-specific legislations. This has been clearly provided by stating that the provisions of this Bill will not be over and above provisions of other Acts, except to the extent of conflict with the provisions of the Bill.

***