

Highlights of the Data Protection Bill, 2019

INTRODUCTION

While the citizens of the country are busy debating the issues, which have come across due to the Citizen (Amendment) Act, 2019, the government introduced a new bill in the Lok Sabha called The Personal Data Protection Bill, 2019 (“Bill”) on December 11, 2019. The Bill has been a topic of debate because even though it talks about “the privacy of individuals relating to their personal data”, it nullifies such privacy by empowering the government to dilute any sort of data protection provisions for any of its agencies thereby giving full access to an individual’s data.

HIGHLIGHTS OF THE BILL

Aims and Objectives

The Bill aims to regulate the processing of personal data of individuals (referred to as “Data Principals” in the Bill) by government and private entities (“Data Fiduciaries”) incorporated in India and abroad. Processing of data is allowed only if the Data Principal gives consent or in a medical emergency, or by the State for providing benefits.

Territorial applicability

The Bill applies to (i) government and private entities incorporated in India; and (ii) entities incorporated overseas, if they systematically deal with Data Principals within the territory of India.

Classification of Data

The Bill provides for classification of data into three types – personal data, sensitive personal data and critical personal data. This distinction forms the basis for providing restrictions on the processing, storage and accessibility of data by Data Fiduciaries.

Rights of a Data Principal:

The Bill prescribes certain rights of the Data Principal whose data is being processed:

- (i) Right to confirmation and access: Confirmation from a Data Fiduciary of whether or not their data has been processed along with access to such data;
- (ii) Right to correction: Correction of discrepancies in such processed data;
- (iii) Right to data portability: Transfer of such data to a different Data Fiduciary; and
- (iv) Right to be forgotten Restriction on use of such data by a Data Fiduciary.

Formulation of Data Protection Authority

The Bill provides for the establishment of a Data Protection Authority (“DPA”) which is empowered to draft specific regulations relating to data protection for all Data Fiduciaries across various sectors, monitor and supervise Data Fiduciaries,



assess compliance with provisions of the Bill and initiate enforcement measures, and receive, handle and redress complaints from Data Principals. The DPA shall consist of a chairperson and 6 members, with knowledge of at least 10 years in the field of information technology and data protection.

Exemptions:

The Bill prescribes exemptions to certain data processing activities by Data Fiduciaries. It states that processing of an individual's personal data will not be subject to the obligations specified, and the Data Principal will not have the rights defined in the Bill, if their personal data is processed for the purposes of national security, prevention, detection, investigation and prosecution due to contraventions of law, legal proceedings, personal or domestic purposes, and journalistic purposes.

The only restrictions on data processing for these purposes are those of (i) processing personal data in a fair and reasonable manner; and (ii) ensuring appropriate security safeguards while processing the data.

ANALYSIS

Although, the proposed Bill, which is largely inspired by European Union's General Data Protection Regulation (GDPR) (which was adopted in 2016 and enforced in 2018), claims to place an individual's rights at the centre of data protection, it does not specify any principles or guidelines for what constitutes a 'fair and reasonable' manner of personal data processing.

According to the Bill, Data Fiduciaries (including the State) cannot process an individual's data without their consent.

However, it also provides for situations wherein such consent would not be required. This becomes a point of concern as the DPA can use such discretionary power to adopt practices of a surveillance state.

The Bill also provides for several restrictions on the processing of data and prescribes a mechanism for the Data Principal to raise a complaint only if there is a violation of the provisions of the Bill. However, it is the responsibility of the Data Principal to demonstrate and prove that harm has been caused to them by unlawful data processing.

Justice B.N. Srikrishna, whose committee's report forms the basis of the Bill has used words such as "Orwellian" and "Big Brother" in reaction to the removal of safeguards for Government agencies and granting them such immense power. This present draft of the Bill comes as a disappointment especially after the emphatic judgment by the Supreme Court on the Right to Privacy.

CONCLUSION

The Bill was referred to the Joint Parliamentary Committee in December 2019. The 30-member committee headed by Ms. Meenakshi Lekhi has invited suggestions from stakeholders and is expected to furnish its report to the Lok Sabha by the second week of the Monsoon Session of Parliament. The Bill has received mixed reactions from the public at large and is both, widely criticised as well as welcome by the companies due to its alignment with GDPR. However, for now, the Bill only lists a set of broad principles that will lay down the outlines for privacy laws in the country. On one hand, certain changes made to the draft Bill may prove to increase ease of doing business as being



in line with the GDPR, however it raised concerns on the subject of privacy of individuals and grant of power to the government to process sensitive information without any check.

***Disclaimer:** This article is meant for informational purpose only and does not purport to be advice or opinion, legal or otherwise, whatsoever. Pioneer Legal does not intend to advertise its services through this article.*