Decoding the Personal Data Protection Bill, 2019: A new data governance framework for India | Ikigai Law

The Personal Data Protection Bill, 2019 ("**Bill**") was introduced in the Lok Sabha (lower house of the Indian Parliament) on 10 December 2019. Once enacted, this Bill will require a large number of companies (both Indian and foreign) to revamp their operational practices. This post provides an overview of the major practical concerns raised by this Bill.

1. Who is affected by this Bill?

In addition to Indian companies, the Bill applies to: (i) companies that process data in India, (ii) companies outside India that process data in connection with a business in India, and (iii) companies outside India that process data in connection with any activity which involves profiling of people within the territory of India. Therefore, even businesses outside India can be covered by this Bill.

2. Will the Bill change how companies should treat personal data?

The Bill lays down standards for how companies should process personal data, and imposes obligations on them for this purpose. Processing in this context means the use, collection, recording, organisation, storage, alteration, indexing, disclosure and erasure of personal data, amongst other things. Since many tech companies perform these operations on personal data, they will be required to comply with the new obligations under this Bill. Operationalising the privacy framework under the Bill will require companies to make significant changes to their data collection and processing practices. For example, companies will now need to take fresh consent from their users for processing their data, as per the detailed consent requirements under the Bill. Companies will also need to prepare a 'privacy by design' policy. This policy should describe: business practices and technical systems adopted to protect personal data, strategies to anticipate and avoid 'harm' to individuals, and how individuals' interests are accounted for at every stage of data-processing.

3. What about non-personal data?

The Bill allows the government to direct companies to share anonymised personal data/non-personal data for improving service delivery or formulating policies. Non-personal data is defined as any data other than personal data.

4. Does the Bill restrict cross-border transfers of data?

Companies will not be able to freely store and transfer all types of personal data outside India once the Bill is enacted. Some types of personal data, which will be classified as critical personal data by the government, must be stored in

India, and can only be transferred in limited cases (eg., for emergency/ health purposes). Sensitive personal data must also be stored in India, though it can be transferred outside India subject to certain conditions being met.

5. Will companies need to change the manner in which they obtain user consent for processing personal data?

The current data protection framework in India requires companies to obtain user consent for data processing only where sensitive personal data (eg., financial data) is involved. Collection and processing of personal data does not need consent, and consent need not be obtained through a notice. This will change if the Bill is enacted in its current form. This is because the Bill requires companies to acquire user consent in order to process even their personal data (for eg., names, addresses, age etc.). In order to be considered valid, consent must be freely given, informed, specific, capable of being withdrawn and indicated through affirmative action (meaning that 'pre-checked' consent boxes may no longer work). While seeking user consent, companies will have to provide users with detailed notices at the time of collection of data. Additionally, companies cannot make the provision of any good/services or their quality conditional on consent. Thus, access to websites or user registration cannot be made conditional on consent, unless the data to be collected is necessary for the provision of such services.

6. Should companies be concerned by the classification of sensitive personal data under the Bill?

All financial data, health data, biometric data, genetic data, data indicating religious/political beliefs/sexual orientation or caste/tribe status are considered sensitive personal data under the Bill. The Bill imposes stricter standards for processing such data as compared to the standards under India's current data protection framework. For example, companies collecting or processing such data will need explicit user consent – meaning that they will have to inform users of the consequences of processing their data and inform them of processing which is likely to cause them significant harm, in addition to the regular notice and consent requirements. This can have impractical effects for the everyday use of publicly information like surnames that reveal caste/tribe or statements reflecting political/religious opinions available online – it appears that companies will need users' explicit consent for collection and use of even this freely available data.

7. Will the Bill affect how companies should treat children's personal data?

The current data protection framework does not impose additional requirements on companies that process children's data. Once the Bill is passed, companies will have to seek parental/guardian consent and verify children's age before processing their data.

8. Are there any restrictions on the amount of data that can be

collected by companies?

The Bill allows companies to collect personal data only for purposes that are clear, specific, lawful and communicated in advance. Additionally, companies must only collect data that is necessary for processing. This could create difficulties – it may not always be possible to determine the exact purpose of data collection beforehand. For instance, with devices that work in an Internet of Things (**"IoT"**) ecosystem, the purposes for which data may be used are constantly evolving, and so it could be difficult to spell out exactly what purpose the data is going to be collected for.

9. Does the Bill apply different standards to different companies?

The Bill allows the government to notify certain companies as 'significant data fiduciaries' based on factors like the volume of personal data they process, the sensitivity of such data, their turnover etc. Once classified as significant data fiduciaries, companies will have to comply with heightened obligations like conducting data protection impact assessments, appointing data protection officers, and in the case of social media companies, enabling their users to voluntarily verify their accounts. This means that large companies that process large volumes of personal data and enjoy high turnovers can be notified as significant data fiduciaries which will have to comply with these heightened obligations.

10. Does the Bill allow for innovation in emerging technologies that involve the use of data?

The Bill allows the Data Protection Authority to create a data sandbox for the purpose of encouraging innovation in artificial intelligence, machine learning or any other emerging technology in public interest. Companies participating in the sandbox will be able to avail of certain exemptions.

11. Who will regulate this new law?

The Data Protection Authority will be responsible for the enforcement of the Bill once it is enacted. It has wide-ranging powers – including the power to require certain entities to conduct mandatory data protection impact assessments and the power to permit cross-border transfers in certain cases.

12. What are the consequences of non-compliance with the Bill?

Non-compliance with the Bill can attract penalties of up to INR 15 crores or 4% of worldwide turnover, whichever is higher.

[This post has been authored by Tuhina Joshi, Associate, Ikigai Law, with inputs Sreenidhi Srinivasan, Senior Associate, Ikigai Law.]