

# Data protection thorny issue not just for tech, but other industries as well

The proposed Bill will impact not just technology companies, but everyone from your local "kirana" store to the hotel you check into when you're on a holiday. The criminal liability prescribed in the Bill, as well as lack of clarity on certain provisions have been flagged by different industries.

Neha Alawadhi@alnehaa



India's data protection Bill has been in the eye of a storm ever since it was submitted to the government by a Committee headed by Justice Srikrishna.

Apart from the issues associated with the requirement for [data localisation](#), which is likely to increase the costs and the burden of compliance on small and large firms, there are other issues that have been flagged by different industries.

While a large part of the focus has been on technology firms, in its current form however, the Bill will be applicable to a host of other industries from finance to aviation, manufacturing to healthcare.

"The law may be targeted towards big tech (companies), but even if you are a small "kirana" (grocery) store guy using a computer to store your customer's number, the same law will be applicable to him," said Pratibha Jain, partner at law firm Nishith Desai Associates.

As an example, Jain said any company that collects the data of employees will also be impacted by the provisions in the Bill.

"Suppose the employer decides to conduct a diversity survey. According to the Bill in its current form, it requires the company to use the data only for the purposes you have taken consent for. If the company conducts this survey without explicit consent, it will be criminally liable," she added.

The Personal Data Protection Bill, 2018 was presented to the Ministry of Electronics and Information Technology (MeitY) on July 27. After a public outcry over the lack of consultation with various stakeholders, MeitY on August 14 invited public comments on the Bill until September 10. This deadline was extended to September 30, and has now been extended until October 10.

The debate has largely focused around how technology companies and startups use data, but other sectors are now beginning to realise the repercussions for their businesses.

Aviation for example, captures a lot of data. During international travel, in addition to the regular traveller details and financial transaction related information, additional details such as passport information, sometimes medical details and information about next of kin also get captured.

Also, at airports, images or videos also get captured through CCTV footage and there is an increasing use of biometrics as well.

"In the data protection Bill in its current form, management and compliance of data will require time and cost. The Bill currently appears very harsh on every instance of non compliance. That needs to be treated better," said Paramprit Singh Bakshi, VP, South Asia at CAPA India, an aviation advisory and research firm.

The obtaining, transfer, sale or disclosure of personal and sensitive personal data as specified in the Bill, can attract a monetary fine and imprisonment of up to three or five years.

Similarly, in the financial services industry, as well as lending, some concerns have been flagged.

The Bill allows a person to withdraw consent for processing any of their personal data collected by a person or entity who will decide how personal data collected will be processed or acted upon.

"In lending, for example, the Bill allows for a customer to give partial consent. Suppose a customer is sharing eight information items for lending. Now if they want to withdraw consent for one or two of these permissions, it may not be possible to provide credit. Does that constitute denial of service?" asked Alok Mittal, Managing Director, Indifi Technologies Private Limited, a platform for enabling debt financing for small businesses.

Mittal also said criminal liability was an issue and that the Bill leaves a lot of room for interpretation.

Similarly, hotels, airlines, [retail](#) and other industries that offer loyalty programmes would find it tough to comply with the requirements of compliance.

Besides, seeking consent every time personal data is processed would hinder the customer experience.

"The law should allow for some sort of breather or a waiver during the initial transition period," suggested Singh.