Key aspects of the Personal Data Protection Bill, 2019

India's Personal Data Protection Bill has been introduced in the Parliament's lower house, the Lok Sabha, and is likely to be sent to a Joint Parliamentary Committee, comprising of 30 members (20 from the Lok Sabha, 10 from the Rajya Sabha). After the committee makes its recommendations, it will be tabled in the Lok Sabha for passing, after which it will be sent to the Rajya Sabha (the upper house of Parliament) for passing, and then to the President for his assent before it becomes a law.

This law has been two years in the making, and will lead to the creation of a Data Protection Authority in India, the imposition of norms on collecting and processing of data, as well as the cross-border transfer of data. Key aspects of the bill:

1. Kinds of personal data:

The Bill regulates 3 categories of data – Personal Data, Sensitive Personal Data, and Critical Personal Data.

- Sensitive personal data may be transferred for processing outside India with the user's explicit consent and the Data Protection Authority's or Central government's permission , but needs to be stored only in India. Sensitive personal data includes financial data, health data, sexual orientation, transgender status, case/tribe, and religious or political beliefs. The Central government and DPA can together also notify further kinds of data as sensitive personal data. "Passwords" have been removed from the list of sensitive personal data listed in the bill.
- Critical personal data has not been defined and what it is will be notified by the Central government; it can be processed only in India.

The Bill dilutes data localisation requirements, as envisaged in the Srikrishna draft bill, and mandatory mirroring of personal data has also been removed.

2. Right to be Forgotten

The Bill gives a user the right to be forgotten, that is to stop their data from being disclosed if the purpose of data collection has been served, if the user withdrew consent, or the data was disclosed illegally. The user can make a complaint to Data Protection Authority, who will then order the data fiduciary to remove the user's data.

3. Significant Data Fiduciaries

The Data Protection Authority can notify any data fiduciary as a significant data fiduciary on the basis of the volume and sensitivity of personal data being processed, the data fiduciary's turnover, risk of harm by processing by the data fiduciary, use of new technologies for processing, any other factor causing harm from such processing.

A significant data fiduciary will have to carry out a Data Protection Impact Assessment, in order to undertake any processing involving new technologies, use of sensitive personal data such as biometric data, etc. Such a fiduciary also has to undergo compliance evaluation by a data auditor, who is appointed by the Data Protection Authority.

4. Social media intermediaries and verification

If any "social media intermediary" has a certain number of users, and can impact electoral democracy, India's security, sovereignty or public order, can be notified by the Central government and DPA as a "significant data fiduciary". Different thresholds will be notified for different classes of social media intermediaries. A social media intermediary has been defined as "an intermediary who primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services". This does not include intermediaries which enable commercial or business transactions, provide access to the internet, email services, search engines, and online encyclopedias.

Social media intermediaries, classified as significant data fiduciaries, will now have to give **account verification options to willing users**, and **such users will be given a visible mark of verification.** This will be voluntary.

5. Non-personal Data

The bill empowers the Central government to direct any data fiduciary or processor to provide anonymised personal data or other non-personal data "to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government".

6. Consent manager

The bill introduces the concept of consent manager; users can use it to give or withdraw consent to the data fiduciary. Consent manager is defined as a data fiduciary "which enables a data principal to gain, withdraw, review, and manager his consent through an accessible, transparent, and interoperable platform".

7. Personal Data

Personal data's definition has been expanded to include online and offline data about a natural person, "or any combination of such features with any other information", and to include any "inference drawn from such data for the purpose of profiling".

8. Exemptions to the government

The Indian government can exempt any government agency from the Act for reasons of national security, integrity & sovereignty, public order, friendly relations with foreign states, and for preventing any cognizable offence relating to the above.

Apart from exemptions to government agencies, certain rights of users will be suspended if personal data is processed for law enforcement, judicial reasons, journalism, and for personal reasons.

9. Data Protection Authority

The independence of the regulator has been significantly reduced, in comparison with the last bill. The selection committee — which will make recommendations to the government on appointment of DPA's members — are now made up of government officials, including the Cabinet Secretary, Law Secretary, and MeitY secretary. In the earlier version of the bill, this committee consisted of members of the judiciary, including the Chief Justice of India as chairperson. Users have the right to appeal to the Appellate Tribunal, if they are dissatisfied with orders made by an officer of the Data Protection Authority.

10. Processing without consent:

Personal data may be processed without consent for performance of a state function, including for provision of state services and in response to medical emergency, for employment-related purposes. Personal data can also be processed without consent for other "reasonable purposes", including for prevention of illegal activities, whistle-blowing, credit scoring, debt recovery, and importantly – operation of search engines.

11. Children's data privacy:

Data fiduciaries can process a child's personal data only after verifying their age, and obtaining the consent of their parent or guardian. The Data Protection Authority can classify any data fiduciaries who operate services directed at children, or process large amount of children's personal data as a "guardian data fiduciary".

A guardian data fiduciary will be barred from profiling, tracking or monitoring the behaviour of children, target ads at children, or carry out any other processing that can cause significant harm to the child.

Follow our live-blog and Twitter handle for updates.