

## **Personal Data Protection (PDP) Bill, 2019**

### **Why in news?**

The Personal Data Protection (PDP) Bill, 2019, has been approved by the Cabinet and is to be placed in Parliament.

### **How important has 'data principal' become?**

- The individual whose data is being stored and processed is called the 'data principal' in the PDP Bill.
- It usually refers to information about one's messages, social media posts, online transactions, and browser searches.
- This large collection of information about one's online habits has become an important source of profits.
- On the other hand, it is also a potential avenue for invasion of privacy because it can reveal extremely personal aspects.
- Thus, companies, governments, and political parties find it valuable as it offers the scope for having the most convincing ways to advertise online.
- Certainly, much of the future's economy and law enforcement will be based on data regulation, introducing issues of national sovereignty.

### **How is data handled and processed?**

- Data is collected and handled by entities called data fiduciaries.
- While the fiduciary controls how and why data is processed, the processing itself may be done by a third party, the data processor.
- This distinction is important to delineate responsibility as data moves from entity to entity.
- E.g. in the US, Facebook (the data controller) fell into controversy for the actions of the data processor, [Cambridge Analytica](#)
- The physical attributes of data - where data is stored, where it is sent, where it is turned into something useful - are called data flows.
- Data localisation arguments are premised on the idea that data flows determine who has access to the data, who profits off it, who taxes and who "owns" it.
- However, many contend that the physical location of the data is not relevant in the cyber world.

## How does the PDP Bill propose to regulate data transfer?

- To legislate on the topic, the Bill trifurcates personal data.
- The umbrella group is all personal data, which is data from which an individual can be identified.
- Some types of personal data are considered sensitive personal data (SPD).
- The Bill defines as SPD, the data on finance, health, sexual orientation, biometric, genetic, transgender status, caste, religious belief, and more.
- Another subset is critical personal data.
- The government at any time can deem something critical, and has given examples as military or national security data.
- In the Bill approved by the Cabinet, there are 3 significant changes from the version drafted by the Justice B N [Srikrishna Committee](#).

## How does the Bill differ from the earlier draft?

- **Localisation** - The draft had said all fiduciaries must store a copy of all personal data in India.
- This was criticised by foreign technology companies that store most of Indians' data abroad.
- The approved Bill removes this stipulation, only requiring individual consent for data transfer abroad.
- Similar to the draft, however, the Bill still requires sensitive personal data to be stored only in India.
- It can be processed abroad only under certain conditions including approval of a Data Protection Agency (DPA).
- The final category of critical personal data must be stored and processed in India.
- **Information** - The Bill mandates fiduciaries to give the government any non-personal data when demanded.
- Non-personal data refers to anonymised data, such as traffic patterns or demographic data.
- The previous draft did not apply to this type of data, which many companies use to fund their business model.
- **Social media companies** - Some social media companies are deemed to be significant data fiduciaries based on factors such as volume and sensitivity of data and their turnover.
- The Bill requires these companies to develop their own user verification mechanism.
- The process can be voluntary for users and can be completely designed by the company.
- However, it will decrease the anonymity of users and "prevent trolling."

## What are the other key features?

- The Bill includes exemptions for processing data without an individual's consent for "reasonable purposes".
- This includes security of the state, detection of any unlawful activity or fraud, whistle-blowing, medical emergencies, credit scoring, operation of search engines and processing of publicly available data.
- The Bill calls for the creation of an independent regulator DPA, which will oversee assessments and audits and definition making.
- Each company will have a Data Protection Officer (DPO) who will cooperate with the DPA for auditing, grievance redressal, recording maintenance and more.

**Source: Indian Express**

**Related Article:** [White Paper on Data Protection Framework](#)

