011-45586829 9540226688
9718793363 info@guidanceias.com
OFFICE: 3-B, 4th Floor, Croma Building, Pusa Road, Opp. Pillar No. 108, Karol Bagh Metro Station, New Delhi – 5
website : www.guidanceias.com

The Draft Data Protection Bill

Syllabus-GS 2: *Government Policies and Interventions for Development in various sectors and Issues arising out of their Design and Implementation*

Why in news- The Joint Committee of Parliament that studied the proposed Personal Data Protection Bill & is believed to have adopted a final set of recommendations. The draft Bill is set to be tabled in Parliament's Winter Session.

Why does India need a data protection law?

- Amid the proliferation of computers and the Internet, consumers have been generating a lot of data, which has allowed companies to show them personalised advertisements based on their browsing patterns and other online behaviour.
- Companies began to store a lot of these datasets without taking the consent of the users, and did not take responsibility when the data leaked.
- To hold such companies accountable, the government in 2019 tabled the Personal Data Protection Bill for the first time.

➢ **Applicability:**

The Bill governs the processing of personal data by:

- government,
- companies incorporated in India, and
- foreign companies dealing with personal data of individuals in India.

➢ **Personal data** is data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual.

➢ The Bill categorises certain personal data as **sensitive personal data**. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government.

➢ **Rights of the individual:** The Bill sets out certain rights of the individual. These include the right to:

(i) obtain **confirmation from the fiduciary** on whether their personal data has been processed,

(ii) **seek correction** of inaccurate, incomplete, or out-of-date personal data,

(iii) have **personal data transferred** to any other data fiduciary in certain circumstances, and

(iv) **restrict continuing disclosure of their personal data by a fiduciary**, if it is no longer necessary or consent is withdrawn.

What is data fiduciary:

➢ A data fiduciary is an **entity or individual** who decides the ***means and purpose*** of ***processing personal data***.

- Such processing will be subject to certain purpose, collection and storage limitations.
- All data fiduciaries must undertake certain transparency and accountability measures such as:
  - implementing **security safeguards** (such as data encryption and preventing misuse of data), and
  - instituting **grievance redressal mechanisms** to address complaints of individuals.
- They must also **institute mechanisms for age verification and parental consent** when processing sensitive personal data of children.

- The Bill sets up a **Data Protection Authority** which may:
  - take steps **to protect interests** of individuals,
  - **prevent misuse** of personal data, and
  - **ensure compliance** with the Bill.
- **Transfer of data outside India:** Sensitive personal data may be transferred outside India for processing if explicitly consented to by the individual, and subject to certain additional conditions. However, such sensitive personal data should **continue to be stored in India**. Certain personal data notified as critical personal data by the government can only be processed in India.
- **Exemptions:** The central government can exempt any of its agencies from the provisions of the Act:
  - in interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states, and
  - for preventing incitement to commission of any cognizable offence (i.e. arrest without warrant) relating to the above matters.
- **Sharing of non-personal data with government:** The central government may direct data fiduciaries to provide it with any:
  - non-personal data and
  - anonymized personal data (where it is not possible to identify data principal) for better targeting of services.

The story so far:

- The Joint Parliamentary Committee (JPC) constituted to examine India's proposed data protection law, the Personal Data Protection Bill, 2019, released its report on Monday.

Criticism of draft:

- It contains a number of suggestions that could strengthen the final law, such as:
  - A recognition that promotion of the **digital economy cannot take precedence over the protection of citizen rights**.

DO YOU KNOW

- A Joint Parliamentary Committee (JPC) is an **ad-hoc body** set up to examine a particular bill presented, or for the **purpose of investigating cases** of financial irregularities in any government activity.
- Members are drawn from both the houses.
- So far, the JPC have been set up **7 times** to probe various matters including the **Bofors Contract in 1987**, **2G spectrum** scam in 2011, **VVIP Chopper Scam in 2013**.
- The last time a committee was set up in 2015 for Land Acquisition Bill .

011-45586829 9540226688
9718793363 info@guidanceias.com
OFFICE: 3-B, 4th Floor, Croma Building, Pusa Road, Opp. Pillar No. 108, Karol Bagh Metro Station, New Delhi – 5
website : www.guidanceias.com

- **What is the State exempt from?**
  - The **State is one of the biggest processors of data**, and has a unique ability to impact the lives of individuals, not least due to its monopoly over coercive powers as well as its obligation to provide welfare and services.
  - Draft, permits the **Central Government to exempt any agency of the Government from the provisions of the law**. This is a very wide power that enhances the significant asymmetry in the relationship between the citizen and the State.
  - As demonstrated by the **Pegasus case** or indeed the instances of **privacy violations concerning COVID-19-related interventions**, the current frameworks for protecting citizens from arbitrary and intrusive State action lack robustness.
- **What are the best practices followed in the world?**
  - The JPC recognises that **balancing privacy interests with those of public needs (such as that of State security) is difficult**. However, it falls short of engaging with international precedents.
  - For instance, the JPC notes that the **European GDPR (General Data Protection Regulation)**, exempts from its ambit certain types of processing carried out in public interest (such as for law enforcement purposes).
  - It, however, ignores the fact that first, **EU law typically does not engage with issues concerning national security** (implying that armed forces and intelligence agencies are usually not regulated by EU law), and second, that the **EU has in place a separate law** that deals with the processing of personal data by law enforcement agencies.
  - Accordingly, **countries do put in place regulations concerning processing of personal data by law enforcement agencies**. For example, the U.K.'s Data Protection Act dedicates Part 3 to dealing with law enforcement processing and in this context, **liberalises certain obligations while at the same time ensuring that data protection rights are also protected.**