Personal Data Protection Bill, 2019

The Personal Data Protection Bill, 2019 is an important current affairs topic for the UPSC exam. It is a part of the Governance section of the General Studies Paper II and also can be a part of the Security segment of the General Studies Paper III. In this article, you can read all about the Personal Data Protection Bill, 2019 and related privacy issues for the UPSC exam.

Personal Data Protection Bill - Introduction

The Personal Data Protection (PDP) Bill, 2019, was introduced in the Lok Sabha and is now referred to a joint select committee.

Why is the law important?

- Collection of information about individuals and their online habits has become an important source of profits, but also a **potential avenue for invasion of privacy** because it can reveal extremely personal aspects.
- Companies, governments, and political parties find it valuable because they can use it to find the most convincing ways to advertise online.
- To prevent the breach of privacy and unwarranted advertising, this bill was a necessity.

Related Terms Explained

Data

- Data is any collection of information that is stored in such a way that computers can easily read them.
- Data usually refers to information about an individual's messages, social media posts, online transactions, and browser searches.

Data Processing

- The analysis of data to collect patterns, turning raw data into useful information.

Data Principal

- The individual whose data is being collected and processed.

Data Fiduciary

- The entity that collects and/or processes a data principal's data.

Data Processor

- The entity that a fiduciary might give the data to for processing, a third-party entity.
- The physical attributes of data — where data is stored, where it is sent, where it is turned into something useful — are called data flows.

Personal Data

- It is data which pertains to characteristics, traits or attributes of identity, which can be used to

identify an individual.

Sensitive Personal Data

- Data related to finances, health, official identifiers, sex life, sexual orientation, biometric, genetics, transgender status, intersex status, caste or tribe, religious or political belief or affiliation. This data can only be sent abroad with authority approval.

Right to data portability

- The right to receive the data from the fiduciary in a machine-readable format.

The right to be forgotten

- The right to restrict continuing disclosure of personal data.

Data Protection Authority (DPA)

- A government authority tasked with protecting individuals' data and executing this Act through codes of practice, inquiries, audits and more.
- Each company will have a **Data Protection Officer (DPO)** who will liaison with the DPA for auditing, grievance redressal, recording, maintenance and more.

Adjudicating Officers:

- Officers in the DPA with the power to call people forward for inquiry into fiduciaries, assess compliance, and determine penalties on the fiduciary or compensation to the principal.
- Adjudication decisions can be appealed in the appellate tribunal.
- Appeals from the Tribunal will go to the Supreme Court.

Personal Data Protection Bill Features

The Bill seeks to provide for the protection of personal data of individuals.

- The Bill governs the processing of personal data by:
  - Government
  - Companies incorporated in India
  - Foreign companies dealing with personal data of individuals in India
- **Obligations of data fiduciary**: Personal data can be processed only for a specific, clear and lawful purpose. Additionally, 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.
- **Rights of the individual**
  - Seek correction of inaccurate, incomplete, or out-of-date personal data.
  - Have personal data transferred to any other data fiduciary in certain circumstances.
  - Restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn.
- **Grounds for processing personal data:** The Bill allows the processing of data by fiduciaries only if

consent is provided by the individual. However, in certain circumstances, personal data can be processed **without consent**. These include:

- If required by the State for providing benefits to the individual,
- Legal proceedings,
- To respond to a medical emergency.

Exemptions

The central government can exempt any of its agencies from the provisions of the Act:

- In the interest of the security of the state, public order, sovereignty and integrity of India and friendly relations with foreign states, and
- For preventing incitement to the commission of any cognisable offence (i.e. arrest without warrant).

Offences:

- Processing or transferring personal data in violation of the Bill is punishable with a fine of Rs 15 crore or 4% of the annual turnover of the fiduciary, whichever is higher, and
- Failure to conduct a data audit is punishable with a fine of five crore rupees or 2% of the annual turnover of the fiduciary, whichever is higher.

Personal Data Protection Bill - Impact on Organisations

- Private organisations will have a lot to do, from **making technical changes in engineering architecture** to modifying business processes. At the core, they need to place limits on data collection, processing and storage, but there's a lot more.
- **Technical security safeguards, including de-identification—preventing an individual's identity to be inadvertently revealed**—and encryption needs to be built in. Any instance of data breach needs to be reported to the regulator.
- Larger organizations—depending on the volume of data, annual turnover and other factors—and social media companies with users above a **defined threshold will have additional responsibilities**. This includes conducting data protection impact assessments for specific tasks defined by the regulator, periodic security audits and appointing a data protection officer. Additionally, social media platforms would be required to enable users to voluntarily verify their accounts, similar to the "blue tick" on Twitter.

How is it different from the draft?

In the Bill, there are significant changes from the version drafted by a committee headed by Justice B N Srikrishna.

- Data Protection Authority's composition is dominated by the government, as contrasted with the diverse and independent composition as suggested in the committee's **draft**.
  - In the current **bill**, the authority's chairperson and six whole-time members will be appointed on the recommendation of a committee comprising the **cabinet secretary, IT secretary and law secretary**.
- The **draft** had said all fiduciaries **must store a copy of all personal data in India** — a provision that was criticized by foreign technology companies that store most of Indians' data abroad and even some domestic startups that were worried about a foreign backlash.
  - The **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.
- 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.

Personal Data Protection Bill Merits

The merits of the Personal Data Protection Bill are described below.

- All personal data (characteristic, trait, attribute or other feature of the person) online or offline, shall require the **explicit and informed consent of the individual to whom it belongs to** before such data can be collected or subjected to any form of analysis.
- **Section 6** of the Bill provides that any data collected should only be to the extent necessary for the processing of such personal data. **Section 7** mandates that a notice be given to the person whose data is being collected, of the nature and categories of personal data, and the purposes for which the data is to be processed, among other things.
    - This should put a huge spoke in the wheels of organisations that **thrive on processing and monetising data collected from individuals**.
- Data localisation will help law-enforcement access data for investigations and enforcement.
    - As of now, much of cross-border data transfer is governed by individual bilateral "mutual legal assistance treaties" — a **process that almost all stakeholders agree is cumbersome**.
    - In addition, proponents highlight security against foreign attacks and surveillance, harkening notions of data sovereignty.
- Many **domestic-born technology companies**, which store most of their data exclusively in India, support localisation.
    - PayTM has consistently supported localisation.
    - Reliance Jio has strongly argued that data regulation for privacy and security will have little teeth without localisation, calling upon models in China and Russia.
- Many economy stakeholders say localisation will also increase the **ability of the Indian government to tax Internet giants**.

Personal Data Protection Bill Concerns

The concerns of the Personal Data Protection Bill are described below.

- The appointment of members to the DPA will not be made through an independent body but by a handful of people, mostly bureaucrats, selected by the government.
- Civil society groups have criticized the open-ended exceptions given to the government in the Bill, allowing for surveillance.
    - There is a **blanket power of exemption from all provisions of the law** (including access to personal data without consent, citing national security, investigation and prosecution of any offence, public order) in favour of a government agency.
- A new watchdog without teeth, with no functional autonomy, would mean governments are legally immune from charges of data-mining.
    - Justice (Rtd) BN Srikrishna, who headed the committee that formulated the original draft of the Bill, has reportedly called it "a piece of legislation that could turn India into an Orwellian state".
- Technology giants like Facebook and Google and their industry bodies, especially those with

significant ties to the US, have slung heavy backlash.
    - Many are concerned with a fractured Internet where the domino effect of **protectionist policy will lead to other countries following suit**.
    - Much of this sentiment harkens to the values of a **globalised, competitive internet marketplace**, where costs and speeds determine information flows rather than nationalistic borders.
- Allowing the government to force companies to transfer non-personal data **raises serious intellectual property concerns**, and can still threaten users even if they're not individually identified

Comparison of Personal Data Protection (PDP) Bill and General Data Protection Regulation (GDPR)

Where are they alike?

- The **exceptions** given to the Indian Bill and the EU Regulation look similar. Both allow data processing for prevention, investigation, detection, or prosecution of criminal offences. Both also discuss "public security", "defence", and "judicial" proceedings.
    - The GDPR states: "This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as **activities concerning national security**. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the **common foreign and security policy of the Union.**"
- **Consent**: The PDP Bill and the GDPR are founded upon the concept of consent. In other words, data **processing should be allowed when the individual allows it**. Consent carries similar meanings, with words like "free", "specific", and "informed".
- **Individual's rights:** Both have similar rights given to the individual, including the **right to correction, the right to data portability** (transferring your data to another entity), and the right to be forgotten (the right to erase the disclosure of your data).
    - But the right to object to profiling is in the GDPR and not the PDP Bill.
- **Other similarities:** Both place responsibility on the fiduciaries, such as building products that include privacy by their design and transparency about their data-related matters.
    - The European Data Protection Board in the GDPR and the Data Protection Authority in the PDP Bill have **some similar duties, such as dispute resolution and codes of conduct**.

Where do they differ?

- **Data Transfer Abroad:** One significant difference between the GDPR and the PDP Bill is the framework built around deciding whether or not data can leave the country. Both give a government authority the power to decide if data transfers can occur, but the GDPR more clearly lays out the parameters of this decision.
    - Their "**Adequacy Decision**" is made based on the country's rule of law, authorities, and other international commitments. The transfer can be made without this decision if there are legally binding rules or other codes of conduct that allow for it.
    - The PDP simply states that the Authority has to have the approval of the transfer of any sensitive personal data abroad, without specifying as many details about the other country's "adequacy" in receiving the data.
- **Automated Decisions:** The GDPR much more directly addresses personal harm from automated decision-making.
    - The PDP Bill requires an assessment in cases of large-scale profiling but does not give the citizen the right to object to profiling, except in the cases of children.

Conclusion

- The sweeping powers the Bill gives to the Government renders **meaningless the gains from the landmark K.S. Puttaswamy vs. Union of India case**, which culminated in the recognition that privacy is intrinsic to life and liberty, and therefore a basic right. Read more about the right to life.
- The idea of privacy is certainly not reflected in the Bill in its current form and hopefully, the parliamentary committee looks into it and due changes are initiated.