

Digital Personal Data Protection Bill, 2022

[UPSC Current Affairs]

The government came out with a new draft data protection bill in November 2022. The draft bill is out in the public for consultation and feedback. In this article, you can read all about the new data protection bill 2022 for the UPSC exam. Important bills and acts passed by Parliament are very important for the [IAS exam](#) polity and governance segment.

Digital Personal Data Protection Bill, 2022

The government had introduced the [Personal Data Protection Bill, 2019](#) in the Lok Sabha in 2019. However, the bill was withdrawn in August 2022 citing the inadequacy of the provisions in meeting global standards regarding data privacy. The new bill has been introduced after a revamp of the provisions.

The salient features of the draft Digital Personal Data Protection Bill, 2022 are as under.

- The new bill seeks to establish a **Data Protection Board (DPB)** with the purpose to adjudicate on the matter of data protection.
 - It also seeks to establish **Data Protection Officers or independent data auditors by companies of large size with the objective to verify the compliance of the law by the institutions concerned.**
- The data principals (whose data it is) were given additional rights with respect to their personal data. The data principals can ask the companies concerned **to erase or delete their data.**
- This bill **laid an additional layer of obligation or duty on the companies** with respect to data.
 - Companies will not be obligated to keep user data that no longer serves a business purpose.
 - Companies should not process personal data that could harm minors (children under 18 years of age).
- The new data protection law came out with the intention to **provide an additional layer of security to the personal data** of the citizens.
- The new bill also **relaxes the norms related to cross-border data flow** as this was a matter of concern for big tech companies.
- It also **eases compliance requirements for start-ups.**
- The bill also **enumerates the conditions under which proposed legislation can be breached** by the government agencies in case of exigencies like:
 - Sovereignty and integrity of India,

- Security of the state,
- Friendly relations with foreign states,
- Maintenance of public order or preventing incitement to any cognisable offence.
- The right to portability that was provided in the previous version has been done away with.
- The 'deemed consent' has been introduced to cover non-consent-based grounds for processing data.
- There is recognition of [alternate dispute resolution](#) processes like arbitration.
- Hardware certification and algorithmic accountability are also eliminated in the new proposal.
- For the benefit of end users, a sort of deterrent has been provided for data leakages by imposing high penalties in case of a breach.
- Moreover, there is also a provision of consent for data sharing and only when permission is given by the end user, the data can be written.

Significance of the new proposed legislation:

- The proposed bill was brought into being only after a comprehensive review of similar laws in the EU, Singapore, and many other jurisdictions.
- The proposed bill would provide predictability of law and enable the companies to align their policies in consonance with the proposed legislation.
- According to data from the [United Nations Conference on Trade and Development \(UNCTAD\)](#), an estimated **137 out of 194 countries have put in place legislation to secure the protection of data and privacy, with Africa and Asia showing 61% (33 countries out of 54) and 57% adoption respectively.**
- **Only 48% of Least Developed Countries (22 out of 46) have data protection and privacy laws.**

Data protection law in the European Union:

- The General Data Protection Regulation (GDPR) is a data-related law that is applied to companies operating within the European territory.
- In the EU, **the right to privacy is enshrined as a fundamental right** that seeks to protect an individual's dignity and her right over the data she generates.
- The GDPR mechanism applies to the processing of personal data, and to **processing activities carried out by both the government and private entities.**
- It has been criticised for being excessively stringent and imposing many obligations on organisations processing data.
- It also lays down certain exemptions related to the applicability of law, **such as national security, defence, public security, etc.**

Draft Digital Personal Data Protection Bill Concerns

Some of the concerns raised by experts about the proposed data protection bill are discussed below.

- The draft bill provides a **blanket exemption to the security agencies** with respect to complying with the provision of the law.
- Exemptions are granted on the basis of loosely defined terms like **sovereignty and integrity of India, public order, and security of the state**. This can be misused by the authorities.
- The earlier bill had an institution called the Data Protection Authority, it was supposed to be a statutory authority. But, the new bill envisages a board to be appointed by the government. The nature of the Data Protection Board is still not clear. It should be clarified whether it would be a judicial body or an administrative body.
- **Relaxing the data localisation norms** would lead to the misuse of data by foreign nationals.
- The draft will solve the issue of data security only in the primary stage and lacks provision for advanced and complex cases.
- Another challenge associated is the emergence of the metaverse and its probability to impact every aspect of life.
- A single framework for different sectors like e-commerce platforms, health techs, automobile companies, etc. is also a serious concern.

Key changes the government is considering to the proposed data protection Bill after feedback received from a range of stakeholders.

- The government is considering tightening the much-criticised provision of '**deemed consent**' for how private entities can process personal data. There were concerns over the misuse of this provision by private entities, so the government is considering changing the provision to exclude private entities. However, government entities are expected to be allowed to process assuming deemed consent, as has been prescribed in the draft Bill.
- The Bill could also incorporate a provision to ensure it does not come in conflict with pre-existing regulations issued by other Departments or Ministries.
- Under Clause 8 of the original draft, a user is said to have given consent to the processing of her personal data if the same is considered necessary. What the provision essentially means is that if a user has voluntarily shared her data with an entity for a certain purpose, that entity can assume her consent for other adjacent purposes and does not have to seek fresh consent for it.
- The current provision on cross-border data flows, as prescribed under Clause 17 of the draft data protection Bill, states that the Centre will notify countries or territories where the personal data of Indian citizens can be transferred.

- This is likely to be amended with the Bill allowing cross-border data flows to all geographies with an official blacklist — of countries where transfers would be restricted.
- This change is seen as a move to ensure business continuity for enterprises and to place India as a crucial part of the global data transfer network – an important element of trade negotiations the country is currently exploring with key regions such as the European Union.
- If other sectoral laws prescribe a higher standard of data protection on account of national security or other factors, **then the data protection Bill will not supersede them.** If there are sectoral regulations related to, for instance, health where such data is subject to a certain degree of privacy, that regulation will prevail over the data protection Bill.[/su_box]

Conclusion: Data is a new fuel in the modern world. There has been huge competition among companies to gain hegemony over citizens' data. This can seriously enable the companies to manipulate the free will of the citizens. Therefore, the time calls for proper protection and processing of the data based on the prior information given to the user. The new data protection bill has to rise up to this expectation.