



## Data Governance in India

**For Prelims:** [DPDP 2022](#), [GDPR](#), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, Proposal of 'Digital India Act', 2023.

**For Mains:** Data Governance in India.

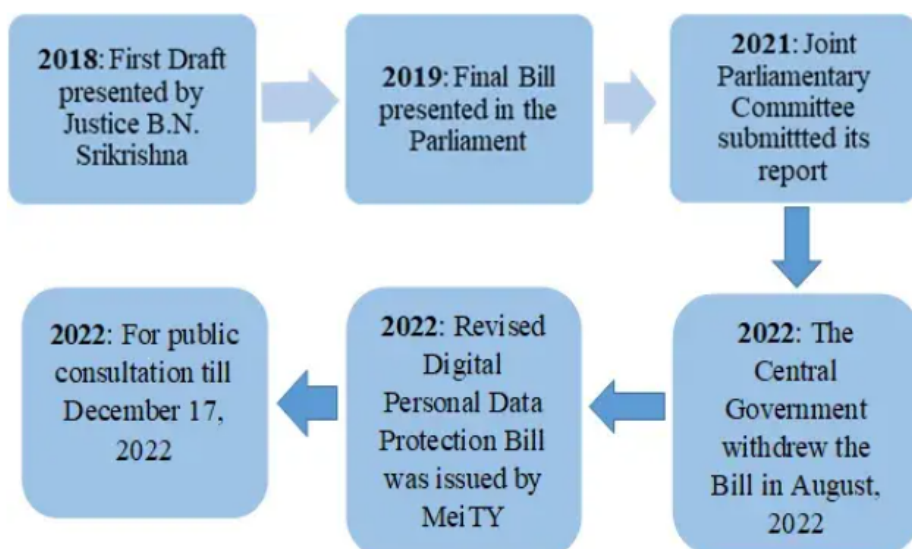
**Source:** [IE](#)

### Why in News?

Recently, the Union Cabinet has approved the [Draft Digital Personal Data Protection Bill \(DPDP\), 2022](#), to introduce in the Monsoon session of Parliament with some significant changes, including lowering the age of consent for data processing and providing exemptions for certain companies.

- If passed, the law will become India's **core data governance framework**, six years after the Supreme Court declared privacy as a fundamental right.
- The Bill is one of the four proposed legislations in the IT and telecom sectors to provide the framework for the rapidly growing digital ecosystem. Other three bills are,
  - [Digital India Bill](#): It aims to replace the [Information Technology Act, 2000](#).
  - [Indian Telecommunication Bill, 2022](#): A new bill related to the telecommunications sector.
  - [Non-Personal Data Governance Policy](#): A policy focused on governing non-personal data.

//



### What are the Expected Changes?

- **Lowering Age of Consent:**
  - The Bill had fixed the age of consent at 18 years, requiring **parental consent for processing data of individuals below 18.**
  - The upcoming Bill will adopt a **graded approach, allowing a case-by-case determination** of the age of consent.
    - The change addresses concerns raised by social media companies, who argued that a fixed age of consent **would disrupt their operations and hinder services targeted at users under 18.**
  - This aligns with data protection regulations in the **European Union and the United States**, where a lower age of consent is prescribed.
- **Definition of a Child and Exemptions:**
  - The definition of child may include **individuals below 18 or a lower age** as determined by the Central Government.
    - In the 2022 draft, the definition of a child was an **“individual who has not completed eighteen years of age”.**
  - Certain entities dealing with children's data **may be exempted from obtaining parental consent** if they can demonstrate verifiably safe data processing practices.
    - The **Ministry of Women and Child Development**, in collaboration with the **Ministry of IT**, will evaluate **platforms' privacy standards for children to grant exemptions.**
- **Relaxations on Cross-Border Data Flows:**
  - The upcoming Bill introduces further relaxations on cross-border data flows, shifting from a **whitelisting approach to a blacklisting mechanism.**
    - The bill **allows global data to flow by default** to all jurisdictions other than a specified negative list of countries where such transfers would be restricted.
  - This change aims to facilitate **data transfers to international jurisdictions**, streamlining the process for businesses.

## What are the Global Regulations Regarding Data Governance?

- **General Data Protection Regulations (GDPR) of European Union (EU):**
  - The GDPR focuses on a comprehensive data protection law for processing of personal data.
  - 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 fines imposed by the GDPR have prompted organizations worldwide to prioritize compliance. Notable companies, including Google, WhatsApp, British Airways, and Marriott, have faced substantial fines.
  - Moreover, the GDPR's **strict norms regarding data transfers to third countries have had a profound influence on data protection** frameworks beyond the EU.
- **Data Governance in US:**
  - There is **no comprehensive set of privacy rights** or principles in the US that, like the EU's GDPR, addresses the use, collection, and disclosure of data.
    - Instead, there is **limited sector-specific regulation.** The approach towards data protection is different for the public and private sectors.
  - The activities and powers of the government vis-a-vis personal information are well-defined and addressed by broad legislation such as the Privacy Act, the Electronic Communications Privacy Act, etc.
    - For the private sector, there are some sector-specific norms.
- **Data Governance in China:**
  - The **Personal Information Protection Law (PIPL)** grants Chinese individuals new rights to protect personal data.
  - The Data Security Law (DSL) categorizes **business data by importance and imposes restrictions on cross-border transfers.** These laws aim to prevent misuse of personal data.

## What are the Challenges with Data Governance in India?

- **Insufficient Awareness:**

- The **limited understanding among individuals** and organizations regarding the significance of data protection and the potential risks linked to data breaches.
- **Weak Enforcement Mechanisms:**
  - The existing legal framework concerning **data protection in India lacks robust mechanisms** for enforcing compliance. This deficiency makes it difficult to hold organizations accountable for data breaches and non-compliance with data protection regulations.
- **Lack of Standardization:**
  - A significant hurdle in implementing and enforcing data protection regulations in India is the **absence of standardized practices among organizations**. The lack of uniformity in data protection protocols poses challenges when attempting to establish and adhere to consistent data protection practices.
- **Inadequate Safeguards for Sensitive Data:**
  - The current data protection framework in **India fails to offer sufficient safeguards for sensitive data**, such as health data and biometric data.
  - As organizations increasingly collect these types of data, the lack of adequate protection measures becomes a concern.

## How is Data Governed in India??

- IT amendment Act, 2008.
- [Information Technology \(Intermediary Guidelines and Digital Media Ethics Code\) Rules 2021](#)
- [Proposal of 'Digital India Act', 2023 to replace IT act, 2000](#)
- [Justice K. S. Puttaswamy \(Retd\) vs Union of India 2017](#)
- B.N. Srikrishna Committee 2017

## Way Forward

- The government should lead by example in prioritizing data protection as it plays a significant role as a data fiduciary and processor.
- Creating an independent and empowered data protection board with parliamentary or judicial oversight is crucial for effective governance and enforcement of data protection regulations.
- Finding the right balance between stringent regulations to safeguard personal data and fostering innovation is essential. Overly prescriptive and restrictive norms can stifle innovation and impede cross-border data flows.

## UPSC Civil Services Examination, Previous Year Questions (PYQs)

### Prelims

**Q1. 'Right to Privacy' is protected under which Article of the Constitution of India? (2021)**

- (a) Article 15
- (b) Article 19
- (c) Article 21
- (d) Article 29

**Ans: (c)**

**Exp:**

- In Puttaswamy v. Union of India case, 2017, the Right to Privacy was declared a fundamental right by the Supreme Court as an intrinsic part of the Right to Life and Personal Liberty under Article 21.
- **Therefore, option (c) is the correct answer.**

**Q2. Right to Privacy is protected as an intrinsic part of Right to Life and Personal Liberty. Which of the following in the Constitution of India correctly and appropriately imply the above statement? (2018)**

- (a) Article 14 and the provisions under the 42nd Amendment to the Constitution.
- (b) Article 17 and the Directive Principles of State Policy in Part IV.
- (c) Article 21 and the freedoms guaranteed in Part III.
- (d) Article 24 and the provisions under the 44th Amendment to the Constitution.

**Ans: (c)**

---

**Mains**

**Q.** Examine the scope of Fundamental Rights in the light of the latest judgement of the Supreme Court on Right to Privacy. (2017)

PDF Reference URL: <https://www.drishtiias.com/printpdf/data-governance-in-india>

