



## Need for Comprehensive Data Protection Laws

This editorial is based on [Ignore GDPR at your own peril](#) which was published in The Hindu Business Line on 01/06/2023. It talks about status of Data protection laws globally and in India.

**Prelims:** [General data protection regulations](#), [Digital Personal Data Protection Bill](#), [IT Act](#).

**Mains:** India's Digital data governance, it's Challenges and Way Forward

In the digital age, the extensive collection and processing of personal data have become the lifeblood of communication and transactions within the digital ecosystem. However, the potential for misuse and abuse of digital technologies has raised significant concerns regarding the protection of personal data. The **European Union's General Data Protection Regulation (GDPR) stands as a prime example of an effective data protection framework.**

India has also been trying to strengthen its data governance through steps such as Digital Personal Data Protection Bill, Information Technology Act (IT Act) of 2000. India also plans to bring Digital India Act to replace IT act, 2000.

### What are the Global Regulations Regarding Data Governance?

- **General Data Protection Regulations (GDPR) of [European Union \(EU\)](#):**
  - The [General Data Protection Regulation](#) 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:**

- New Chinese laws on **data privacy and security** issued over the past 2 years include the **Personal Information Protection Law (PIPL)**, which came into effect in November 2021.
  - It gives **Chinese data principals new rights** as it seeks to prevent the misuse of personal data.
- **The Data Security Law (DSL)**, which came into force in September 2021, requires business data to be **categorized by levels of importance**, and puts new restrictions on cross-border transfers.

## What are the Provisions Related to Data Governance in India?

- **IT amendment Act, 2008:**
  - Existing Privacy Provisions India has some privacy provisions in place under the **IT (Amendment) Act, 2008**.
  - However, these provisions are **largely specific to certain situations**, such as **restrictions on publishing the names of juveniles and rape victims** in the media.
- **Justice K. S. Puttaswamy (Retd) vs Union of India 2017:**
  - In August 2017, a **nine-judge bench of the Supreme Court** in Justice K. S. Puttaswamy (Retd) Vs Union of India unanimously held that Indians have a **constitutionally protected fundamental right to privacy** that is an intrinsic part of life and liberty under [Article 21](#).
- **B.N. Srikrishna Committee 2017:**
  - Government appointed a **committee of experts for Data protection** under the chairmanship of **Justice B N Srikrishna** in August 2017, that submitted its report in July 2018 along with a draft Data Protection Bill.
  - The Report has a wide range of **recommendations to strengthen privacy law** in India including **restrictions on processing and collection of data**, **Data Protection Authority**, [right to be forgotten](#), [data localisation](#) etc.
- **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021:**
  - [IT Rules \(2021\)](#) mandate **social media platforms to exercise greater diligence** with respect to the content on their platforms.
- **Digital Personal Data Protection Bill:**
  - The Bill will apply to the **processing of digital personal data within India** where such data is collected online, or collected offline and is digitised. It will **also apply to such processing outside India**, if it is for **offering goods or services** or profiling individuals **in India**.
  - Personal data may be processed **only for a lawful purpose** for which an individual has given consent. Consent may be deemed in certain cases.
  - **Data fiduciaries will be obligated to maintain the accuracy of data, keep data secure, and delete** data once its purpose has been met.
    - “Data Fiduciary” is defined as any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
  - The Bill grants certain rights to individuals including **the right to obtain information, seek correction and erasure**, and grievance redressal.
  - The central government **may exempt government agencies from the application of provisions of the Bill** in the interest of specified grounds such as security of the state, public order, and prevention of offences.
  - The central government will establish the **Data Protection Board of India** to adjudicate non-compliance with the provisions of the Bill.
- **Proposal of [‘Digital India Act’, 2023](#) to replace [IT act, 2000](#):**
  - IT Act was **originally designed only to protect e-commerce transactions** and define cybercrime offenses, it did not deal with the nuances of the current [cybersecurity](#) landscape adequately nor did it address data privacy rights.
  - The **new Digital India Act envisages to act as catalysts for Indian economy by enabling more innovation**, more startups, and at the same time protecting the citizens of India in terms of safety, trust, and accountability.

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

▪ **Insufficient Awareness:**

- One of the primary obstacles in ensuring data protection in India is **the limited understanding among individuals and organizations** regarding the significance of data protection and the potential risks linked to data breaches. Consequently, individuals may find it **challenging to take the necessary precautions** to safeguard their personal data.

▪ **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.

## What can be the Way Ahead?

- Government as a Role Model Given its significant role as a data fiduciary and processor, the **government must lead by example in prioritizing data protection**.
- Establishing **an independent and empowered data protection board** with parliamentary or judicial oversight is crucial to ensure effective governance.
- **Balancing Innovation and Regulation is important**. While stringent regulations are necessary to safeguard personal data, overly prescriptive and restrictive norms could stifle innovation and hinder cross-border data flows. Striking the right balance is essential **to foster innovation while effectively protecting personal data**.
- A robust data protection law is just one aspect of a broader framework for digital governance. **To ensure comprehensive regulation, cyber security, competition, artificial intelligence, and other relevant areas must also be addressed**. The European Union's approach, encompassing additional instruments such as the Data Act, Digital Services Act, Digital Markets Act, and the AI Act, can provide valuable insights.

**Drishti Mains Question:**

Highlight the challenges faced in implementing robust data governance in India and propose strategies for enhancing data protection in the country.

## 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.

- Right to Privacy is protected as an intrinsic part of the Right to Life and Personal Liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Indian Constitution.
- Privacy safeguards individual autonomy and recognizes one's ability to control vital aspects of his/her life. Privacy is not an absolute right, but any invasion must be based on legality, need and proportionality.
- 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)**

**Explanation:**

- In 2017, a nine-judge bench of the Supreme Court (SC) in its verdict in Justice K.S. Puttaswamy v. Union of India case unanimously affirmed that the Right to Privacy is a Fundamental Right under the Indian Constitution.
- The SC bench held that the privacy is a Fundamental Right as it is intrinsic to guarantee of life and personal liberty as provided under Article 21 of the Constitution.
- The bench also stated that the elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the Fundamental Rights contained in Part III of the Constitution.
- Therefore, option (c) is the correct answer.

---

## **Mains**

**Q.1** 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/need-for-comprehensive-data-protection-laws>