# Perspective: Data Localisation

**For Prelims:** Data Protection, Personal Data, Privacy, Personal Data Protection Bill, Data Localisation, Other Related Laws

**For Mains:** Data Localisation: Advantages, Regarding Concerns, Provisions in India, Steps that can be taken

## Why in News?

Data plays an increasingly important role as an economic and strategic resource. It can be used to make decisions with economic impacts, environmental impacts or effects on health, education or society in general. The volume of data in the world is increasing exponentially.

- As per the **United Nation's digital economy report 2021**, 64.2 zettabytes of data were created in 2020 which is a 314 percent increase from 2015.

## What is Data Localisation?

- **About:**
  - Data Localisation **is storing critical as well as non-critical data** within the territorial boundaries of the country.
  - The most important aspect of data localisation is **having control over our own data** which makes the country more resistant to issues around privacy, information leaks, identity thefts, security etc.
    - It has also helped the countries develop their own startups, evolve locally and also thrive in their own language.
  - The Ministry of Electronics and Information Technology (MeitY) has drafted a **Bill on Protection of Personal and Sensitive Data.**
    - Under the Draft Bill, entities dealing with users' personal data are mandated to store a copy of such data within India and the export of undefined "critical" personal data is prohibited.
      - Personal data includes information- online or offline- that could be used to identify an individual and hence allows profiling that person.
- **Different Variants of Localisation:**
  - There are four key types of localisation variants. These include:
    - Conditional localisation that entails a local storage requirement
    - Unconditional local storage requirements (for all personal data)
    - Unconditional mirroring requirements (for all personal data)
    - The unconditional free flow of data with bilateral/ multilateral agreements for data access and transfers.

## What are the Data Localisation Norms?

- **In India:**
  - **Srikrishna Committee Report:**
    - Atleast one copy of personal data will need to be stored on servers located within India.
    - Transfers outside the country will need to be subject to safeguards.
    - Critical personal data will only be stored and processed in India.
  - **Data Protection Bill 2018:**
    - The right to privacy is a **fundamental right** which necessitates protection of personal data as an essential facet of informational privacy.
    - Establishment of a Data Protection Authority to take steps to protect interests of individuals, prevent misuse of personal data and to lay down norms for cross-border transfer of personal data.
    - The Central Government shall notify categories of personal data as critical personal data that shall only be processed in a server or data centre located in India.
  - **Draft National E-Commerce Policy Framework:**
    - Recommended data localisation and suggested a two-year sunset period for the industry to adjust before localization rules becomes mandatory.
    - Proposes incentives to encourage data localization and grant infrastructure status to data centres.
  - **Boycott of Osaka Track:**
    - At the **G20 summit 2019,** India boycotted the Osaka Track on the digital economy. The Osaka Track pushed hard for the creation of laws that would allow data flows between countries and the removal of data localisation.
  - **Banning of Chinese Mobile Apps:**
    - In 2020, the Indian government announced to ban 59 widely used apps (such as Tik Tok, ShareIt, Cam scanner etc), most linked to Chinese companies. The Ministry of Electronics and
    - Information Technology (MeitY), invoked **Information Technology (IT) Act, 2000** to cite the concerns regarding both data security and national sovereignty associated with these apps.
- **Global:**
  - US law requires defence-related data to be localised, Australia has sectoral regulation for localising health data, Russia mandates localisation of all its **citizens' personal data**, China requires data **concerning critical information infrastructure and important personal information** to be localised, Indonesian law requires localisation of all public services data, and the EU allows for **conditional data transfer.**
  - Many **bilateral and multilateral agreements** exist as well. These include countries committing to identical data protection norms and commitments towards cross-border data transfer and data localisation, examples being the Osaka Track (2019), the **Clarifying Lawful Overseas Use of Data (CLOUD) Act (2018)**, **Comprehensive and Progressive Agreement for Trans-Pacific Partnership (2018)**, Digital Economy Agreement (DEA), (2020), among others.

## What are the Advantages of Data Localisation?

- **Protects Privacy and Sovereignty**: Secures citizens' data and provides data privacy and data sovereignty from foreign surveillance.
  - The main intent behind data localisation is to protect the personal and financial information of the country's citizens and residents from foreign surveillance
- **Monitoring of Laws & Accountability:** Unfettered supervisory access to data will help Indian law enforcement ensure better monitoring.
  - Data localisation will result in greater accountability from firms like Google, Facebook etc. about the end use of data.
- **Ease of Investigation:** Ensures national security by providing ease of investigation to Indian law enforcement agencies as they currently need to rely on **Mutual Legal Assistance Treaties (MLATs)** to obtain access to data.
  - MLATs are agreements between governments that facilitate the exchange of information relevant to an investigation happening in at least one of those countries. India has signed Mutual Legal Assistance Treaty (MLAT) with 45 countries.

- **Jurisdiction & Reduction in Conflicts:** It will give local governments and regulators the jurisdiction to call for the data when required.
    - Minimises conflict of jurisdiction due to cross-border data sharing and delay in justice delivery in case of data breach.
- **Increase in Employment:** Data centre industries are expected to benefit due to localisation which will further create employment in India.

## What are the Disadvantages of Data Localisation?

- **Investments:** Maintaining multiple local data centres may lead to significant investments in infrastructure and higher costs for global companies.
- **Fractured Internet:** Splinternet, where the domino effect of protectionist policy can lead to other countries following suit.
- **Lack of Security:** Even if the data is stored in the country, the encryption keys may still remain out of the reach of national agencies.
- **Impact on Economic Growth**: Forced data localisation can create inefficiencies for both businesses and consumers. It can also increase the cost and reduce the availability of data-dependent services.

## What can be the Way Forward?

- **Long-term Strategy:** There is a need to have an integrated long-term strategy for policy creation for data localisation.
- **Need for Infrastructural Development:** Adequate attention needs to be given to the interests of India's **Information Technology enabled Services (ITeS)** and **Business Process Outsourcing (BPO)** industries, which are thriving on cross-border data flow.
- **Law Enforcement**: Access to data by Indian law agencies, in case of a breach or threat, cannot be dependent on the whims and fancies, nor on lengthy legal processes of another nation that hosts data generated in India.
    - According to the sources, lack of law enforcement is causing issues in the recent **Free Trade Agreement (FTA)** between India and UK.
- **A Way to Crack Cyber Fraud and Crimes:** For this, the country urgently needs a legally backed framework for a collaborative trigger mechanism that would bind all parties and enable law enforcers to act quickly and safeguard Indian citizens and businesses from a fast-growing menace.
- **Ensure Privacy:** All the players involved, including banks, telecom companies, financial service providers, technology platforms, social media platforms, e-commerce companies and the government, need to play a responsible role in ensuring innocent citizens do not undergo the trauma of suffering losses.
- **Responsibility of Participants:** The customer also has a responsibility to maintain basic cyber hygiene, which includes practices and required precautions to keep one's sensitive information organized, safe and secure.