Data Embassies

Why in news?

The International Financial Services Centres Authority (IFSCA), a regulatory body for the GIFT City, is readying a framework for setting up a single window clearance system for data embassies.

What is a data embassy?

- A data embassy is a solution implemented by nation-states to ensure a country's *digital continuity* with particular respect to critical databases.
- It consists of a *set of servers* that store one country's data and are under that country's jurisdiction while being located in another country, the data archives stored are inviolable and thus exempt from search, requisition, attachment or execution.
- **Purpose-** To provide uninterrupted government services, even in challenging circumstances such as natural disaster, military invasion, cyberattacks, geopolitical conflicts etc.,
- **Estonia-** It has a stringent paperless policy and crucial databases existing only in digital format it explored data embassies after cyberattacks disrupted its digital infrastructure.

  Estonia is the world's first data embassy, it entered into agreement with Luxembourg.

- **Diplomatic agreement**- It enables the home country and the host country to establishes *three pillars of sovereignty* on the recovery site

Pillars of sovereignty	About
Data sovereignty	The home country retains access and control over its data, which is protected through encryption keys and not subject to the host country's jurisdiction
Operational sovereignty	The home country has continuous visibility and control over the provider operations and can maintain its services even during extreme scenarios.
Software sovereignty	The home country can choose the technical stack on which it operates, without depending on the provider's software.

What are the advantages of data embassies?

- **Resilience and continuity**- If a country faces extensive denial-of-service attacks or a military invasion that disrupts its data centers, having a backup in a data embassy

abroad allows for swift recovery.

A denial-of-service (DoS) is a type of cyber-attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning.

- **Security**- Data embassies provide data sovereignty while mitigating threats as keeping data localized within a single facility or geographical boundary can pose security risks.
- **Collaboration**- Data embassies foster collaboration among nation-states and stakeholders, they creatively interpret law and technology to protect and backup data effectively.
- **Efficient infrastructure**- Holding data in state-of-the-art data centers managed by service providers in other countries ensures efficient synchronization and service recovery.
- **Cost effective**- Setting up and maintaining data embassies can be cost-effective compared to building and managing redundant infrastructure within the home country.
- **Back up infrastructure**- Countries consider them as a cital back-ups for critical government collected data, copies of which already exist in the territory of the host country.
- **Jurisdiction**- Data embassies like traditional embassies operate as per the law of the country whose data is being stored in the data centre, not that of the host country. Data stored in these centres is also off-bounds from host state access, much like physical embassies.
- **Data security-** Hosting of Data and Information System agreement signed by Estonia and Luxemburg allows the establishment of data embassy along with immunity and inviolability of the data centre premises by any officials from Luxemburg while granting a right of access to authorized representatives of the Republic of Estonia.

Global legal framework for data embassies
• **Estonia**- It entered into a bilateral treaty with Luxembourg in 2017 on the Hosting of Data and Information Systems. • **Bahrain**- In 2018, it passed a legislative decree which encourages foreign parties (both private and public actor) to enter into an agreement with Bahrain to set up data centres there. • **Monaco**- In 2021 Monaco's e-embassy was established in Luxembourg which finalized the storage of the Monaco's sensitive sovereign data. • **India**- In Budget 2023, the government proposed for data embassies in the country to facilitate seamless digital transfers and continuity for other nations.

What are the challenges with data embassy?

- **Legal complexity**- Establishing data embassies involve navigating complex legal framework, it raises crucial questions regarding juridcition, sovereignty and the applicability of local laws.
- **Operational challenges**-It include setting up and maintaining physical infrastructure,

ensuring robust security measures, and addressing communication and coordination between countries.

- **Security risks-** The risk of data breaches or unauthorized access ramins a challenge hence data embassies must have a secure, resilient infrastructure to protect against cyber threats and physical risks.
- **Privacy**- Countries may have differing privacy laws and regulation, hence the data stored must comply with privacy requirement which is critical.
- **International cooperation**- Data embassies require cooperation and trust among nations, establishing bilateral agreements and frameworks can be time-consuming.
- **Public acceptance**- Convincing citizens and stakeholders about the benefits and necessity of data embassies can be challenging.

How India aims to make it as a global hub in data embassies?

- **Policy formulation**- MeitY is reportedly working on formulating a bespoke policy to allow countries and international companies to establish data embassies within Indian territory.
- **Diplomatic immunity**- The proposed policy is expected to offer diplomatic immunity to the data stored within these embassies, shielding it from Indian regulations.
- **Align with data protection legislation**- The policy on data embassies may be integrated into the existing Digital Personal Data Protection Bill, 2022 (DPDP), or drafted separately.
- **National cloud ecosystem**- MeitY aims to develop a national government cloud to store sensitive sovereign data locally, particularly related to national security.
- **State level policies**- Gujarat have introduced policies to attract investment in IT infrastructure including data centres.

What lies ahead?

- By establishing data embassies, India can attract foreign and private sector investments, boost its digital economy, and highlight the quality of its IT sector.
- The initiative can create employment opportunities, contributing to India’s efforts to become a global hub for data storage.

Reference

1. Business Line- India can become a global hub for data embassies
2. PIB- Data embassy

SHANKAR IAS PARLIAMENT
Information is Empowering