Draft Data Empowerment and Protection Architecture: NITI Aayog

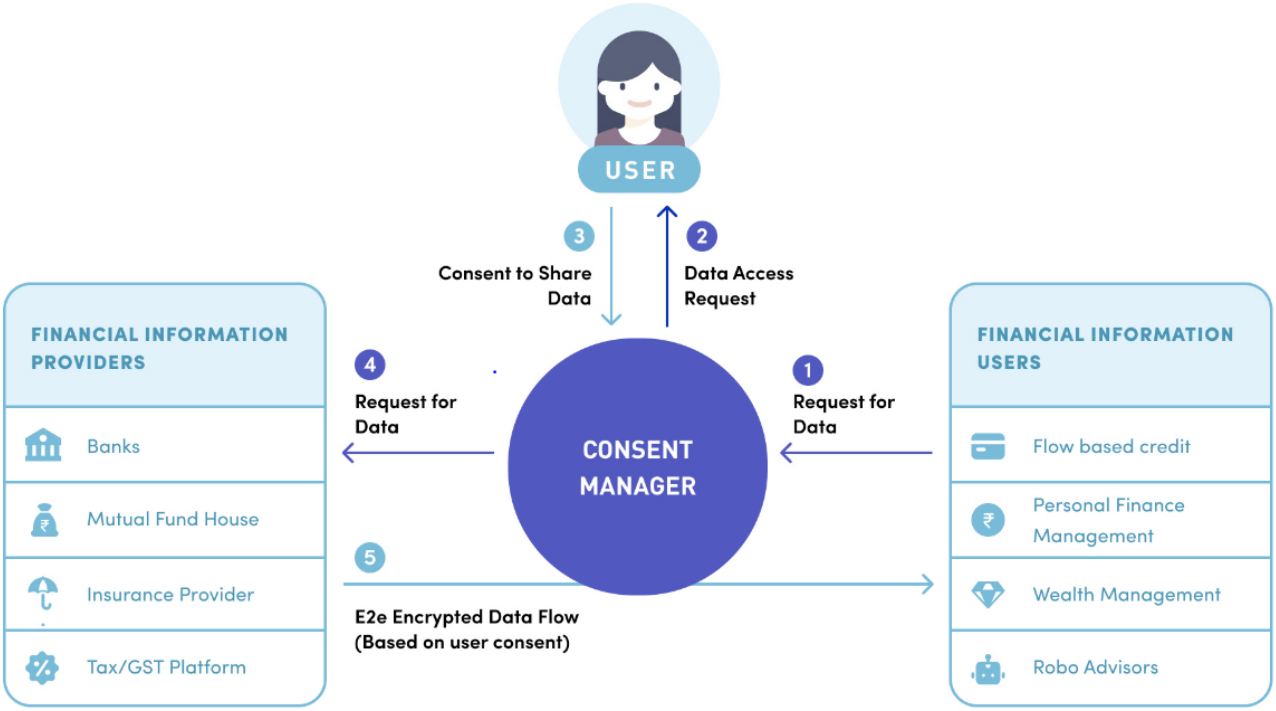
Why in News

Recently, the **NITI Aayog** has released **draft Data Empowerment and Protection Architecture (DEPA)** which aims to promote greater user control on data sharing.

Key Points

- **Features:** DEPA will be empowering individuals with control over their personal data, by operationalising a **regulatory, institutional, and technology design for secure data sharing**.
    - DEPA is designed as an **evolvable and agile framework** for good data governance.
    - DEPA empowers people to **seamlessly and securely access their data and share it with third party institutions**.
    - The consent given under DEPA will be **free, informed, specific, clear, and revocable**.
- **Consent Managers:** DEPA's Institutional Architecture will involve the creation of **new market players** known as User Consent Managers. These will ensure that individuals can provide consent as per an innovative digital standard for every data shared. These Consent Managers will also work to protect data rights.
    - **Reserve Bank of India (RBI)** issued a Master Directive creating Consent Managers in the financial sector to be known as **Account Aggregators (AAs)**. A non-profit collective or alliance of these players is created called the **DigiSahamati Foundation**.
- **Open APIs:** Open **Application Programming Interfaces** (APIs) enable **seamless and encrypted flow of data** between data providers and data users through a consent manager.
- **Implementation:** RBI, **SEBI**, **IRDAI**, **PFRDA** and the Ministry of Finance will implement this model. This regulatory foundation is also expected to evolve with time (eg. with the forthcoming **Data Protection Authority** envisaged under Personal Data Protection Bill**, 2019**).

DEPA Institutional Architecture



//

- **Background:** Regulatory direction on data privacy, protection, consent, and the new financial institutions required for DEPA's application in the financial sector was provided through
    - Supreme Court Judgement on the fundamental **Right to Privacy** in 2017.
    - Personal Data Protection Bill **(PDP), 2019.**
    - Justice Srikrishna Committee Report**, 2018.**
    - RBI Master Direction on NBFC-Account Aggregators**, 2016** (for the financial sector).
- Recently, a government committee headed by Infosys co-founder **Kris Gopalakrishnan** has suggested that **non-personal data** generated in India **be allowed to be harnessed by various domestic companies and entities**.

Application

- **Financial sector:**
    - Using DEPA, individuals and Micro, Small and Medium Enterprises (MSMEs) can use their **digital footprints to access not just affordable loans,** but also **insurance, savings, and better financial management products**.
    - The framework is **expected to become functional for the financial sector starting fall 2020**.
    - It will help in **greater financial inclusion and economic growth**.
    - **Flow based lending:** If **portability and control of data** could allow an MSME owner to digitally share proof of the business' regular tax (GST) payments or receivables invoices easily, a bank could design and offer **working capital loans based on demonstrated ability to repay** (known as flow based lending) rather than only offering bank loans backed by assets or collateral.
- **Telecom Sector:** DEPA is also being launched in the telecom sector following a Telecom Regulatory Authority of India **(TRAI) consultation report on privacy** released in July 2018.
- **Government Departments:** The first major government department to become a Government Information Provider will be Goods and Services Tax **(GST)**.

    - In future, departments with data on individuals and MSMEs could adopt the specifications to improve the ease of doing business or create greater data portability of individual education, jobs, or transaction data.
- **Healthcare:** National Health Authority which has been tasked with implementing the **National Digital Health Mission**, is piloting the DEPA architecture for **healthcare data**.
- **Skilling:** The Ministry of Skill Development and Entrepreneurship is encouraging adoption of a **digital skill credential** that could be used to address low data portability in employment by sharing **verified information on work experience or educational training**.

Advantages

- Opening up an API-based data sharing framework would bring **significant innovation by new** fintech **entities**.
- This architecture **replaces costly and cumbersome data access and sharing practices that disempower individuals,** such as physical submission, username/password sharing, and terms and conditions forms providing blanket consent etc.
- Individuals and small firms do not benefit from individual's data right now. DEPA will provide individuals and small businesses with the practical means to **access, control, and selectively share** personal data that they have stored across **multiple institutional datasets** – to **maximise the benefits of data sharing for individual empowerment whilst minimising privacy risks and data misuse**.
- DEPA will also enable **better personal financial management services, wealth management, robo advisory, or different types of lending, insurance, and investment use cases and products** that one may not be able to foresee today.

Global Approaches to Data Protection and Sharing

- European Union's **General Data Protection Regulation (GDPR)**: It introduces strong data protection laws (through policies such as the right to be forgotten), and the emphasis on gathering minimum data.
- **UK's Open Banking Data Sharing Framework:** It takes a restoration of competition perspective, and mandates that banks work with **Account Information Service Providers** to gather individual **consent** to share data.
- Australia's **My Health Record**, which has an opt-out system rather than a consent-to-share system for health records and the **Australian Consumer Data Right** for the banking sector.
- China's approach has been to create a **tightly controlled internet** that prioritises national security over user control and data democracy.
- The USA has **some cybersecurity measures** but is yet to implement a nationwide data protection law.

Source: IE