DPDP Act, 2023 and DPDP Rules, 2025

For Prelims: Draft Digital Personal Data Protection (DPDP) Rules, 2025, Digital Personal Data Protection (DPDP) Act, 2023, Right to Privacy, Article 21, KS Puttaswamy Judgment, General Data Protection Regulations (GDPR), Data Protection Board of India (DPBI), Telecom Disputes Settlement and Appellate Tribunal, Data Fiduciary, MSMEs.

For Mains: Data privacy and data protection law in India, Key provisions of Data Protection Act 2023 and Draft Digital Personal Data Protection (DPDP) Rules, 2025.

Source: HT

Why in News?

The **Ministry of Electronics and Information Technology (MeitY)** invited **public feedback** on the Draft Digital Personal Data Protection (DPDP) Rules, 2025 for implementing the Digital Personal Data Protection (DPDP) Act, 2023.

- Currently, **stakeholder input** is under review, and the **final rules** are expected to be **enforced soon.**

What is the Digital Personal Data Protection Act, 2023?

- **About:** It is **India's first comprehensive data protection law**, offering a **legal framework** for handling **digital personal data**, with the goal of **safeguarding individual privacy** while permitting **lawful data processing**.
  - Enacted nearly **6 years after** the **Supreme Court's 2017** KS Puttaswamy judgment recognizing **privacy as a fundamental right** under **Article 21**, the Act is inspired by global frameworks like the **EU's** General Data Protection Regulations (GDPR) to outline **privacy** and **data protection obligations**.
- **Applicability:** The Act applies to **digital personal data** processed **within India**, whether **collected digitally** or **digitized later**, and to **data processing outside India** if done for **offering goods or services in India.**
  - It **does not apply** to **personal data** used for **personal purposes** or data **made public** by the **Data Principal** or under a **legal obligation.**
- **Consent: Personal data** can be processed only for a **lawful purpose** with the **consent of the Data Principal**, who may **withdraw consent** anytime. For **children** or **persons with disabilities**, it must be given by a **parent or legal guardian.**
  - Under **Section 9 of the DPDP Act, 2023**, **verifiable parental consent** is mandatory before processing **children's data**, and it **prohibits harmful processing** and **advertising targeting minors under 18 years.**
  - Any user **below the age of 18** has been defined as a **child** under the Act.
  - Consent is **not required** for **legitimate uses** like **government services** or **medical emergencies.**

- **Rights and Duties of Data Principal:** Data Principals (individuals whose personal data is being processed) have the right to **access information**, **request correction or deletion**, seek **grievance redressal**, and **nominate a representative** in case of death or incapacity.
    - They must **avoid false complaints or information**, with violations punishable by a **fine up to Rs 10,000.**
- **Obligations of Data Fiduciaries:** Data Fiduciaries (entity or organization that **collects, stores, processes, or uses personal data** of an individual) must **ensure data accuracy**, implement **security measures** to prevent breaches, and **notify the DPBI and affected individuals** if a breach occurs.
    - They are also required to **erase personal data** once its purpose is fulfilled and retention is no longer legally necessary.
- **Significant Data Fiduciaries (SDF):** The Central Government may designate certain Data Fiduciaries as **SDF** based on factors like **data volume, sensitivity, risk to individual rights**, and threats to **national security, sovereignty, democracy, and public order.**
    - SDFs have extra duties, including appointing a **Data Protection Officer**, an **independent auditor**, and conducting **impact assessments.**
- **Exemptions:** Rights of the data principal and obligations of data fiduciaries **(except data security)** will not apply in specified cases, including:
    - For **notified agencies**, in the interest o**f security, sovereignty, public order**, etc.
    - For **research**, archiving or statistical purposes.
    - Fo**r start-ups** or other notified categories of Data Fiduciaries.
    - To **enforce legal rights and claims**; or Prevention and investigation of offences
    - To perform **judicial or regulatory functions**;
    - To process in India **personal data of non-residents** under foreign contract.
- **Data Protection Board of India (DPBI):** The Act provides for the establishment of the **DPBI** by the **Central Government**, with members appointed for **two years** and eligible for **reappointment**.
    - Its **functions** include **monitoring compliance**, **imposing penalties**, handling **data breach responses**, **hearing grievances**, and appeals can be made to the **Telecom Disputes Settlement and Appellate Tribunal**.

Note: Section 44(3) of the DPDP Act amends **Section 8(1)(j) of the RTI Act**, removing the **"larger public interest"** test. Now, government bodies can **withhold personal information** under RTI requests **without considering public benefit**, simply by labeling it as **personal data.**

What are the Key Provisions of the Draft DPDP Rules, 2025?

- **Data Transfer:** The rules allow the transfer of **certain personal data outside India**, as approved by the government.
- **Data Erasure:** Data retention is allowed for up to **three years** from the last interaction with the **Data Principal** or the effective date of the rules, whichever is **later.**
    - The **Data Fiduciary** must notify the Data Principal **at least 48 hours before erasure.**
- **Digital-First Approach**: The rules also prescribe a **"digital by design" Data Protection Board of India** (DPBI) for consent mechanisms and grievance redressal, for **faster resolution of complaints** and grievances online.
- **Graded Responsibilities:** Graded responsibilities cater to **startups and MSMEs** with **lower compliance** burden, while **Significant Data Fiduciaries** have higher obligations.
    - Digital platforms with a large number of users such as **Facebook, Instagram, YouTube, Amazon, Flipkart, Netflix,** etc, will qualify as significant data fiduciaries.
- **Consent Managers:** The digital platform may also collect consent through **consent managers.**
    - A **Consent Manager** must be an Indian company with a minimum net worth of **Rs 2 crore**, responsible for managing the collection, storage, and use of user consent in data privacy and digital interactions.

What are the Key Concerns Associated with the Digital Personal

Data Protection Act?

- **Excessive State Exemptions**: The Act grants **many exemptions to the State**, enabling **data collection, processing, and retention** beyond necessity, potentially **violating the fundamental right to privacy**.
- **Absence of Crucial Data Rights**: The Act **omits essential rights** like the **right to data portability** (to obtain and transfer one's personal data).
- **Unrestricted Cross-Border Data Flow**: It permits **free transfer of personal data to most countries**, with restrictions only at the discretion of the government—raising **data security and sovereignty concerns**.
- **Lack of Harm Prevention Measures**: The legislation fails to explicitly address **harms such as identity theft, financial fraud, or discriminatory profiling**, leaving data principals vulnerable.

What Measures Can be Adopted to Strengthen DPDP Act, 2023?

- **Clarify Exemption Provisions**: Provide **clear definitions** for terms like **sovereignty** and **integrity of India** and establish a **transparent process for granting exemptions** under the **DPDP Act, 2023**
- **Promote Bilateral Data Agreements**: Support **bilateral and multilateral agreements** to facilitate **safe data exchange**, rather than adopting restrictive or isolationist policies.
- **Ensure Regulatory Flexibility**: Develop a **dynamic and adaptive regulatory framework** that evolves with **emerging technologies** and **new privacy challenges**
    - Form a **specialized task force** to proactively **identify risks** associated with AI and **co-develop responsive data protection strategies.**
- **Adopt Global Best Practices**: Integrate lessons from international models such as the **EU-US data privacy framework** to ensure **secure and trusted cross-border data flows**.

Evolution of Right to Privacy in India

- **AK Gopalan Case, 1950:** The Supreme Court rejected the argument regarding the right to privacy.
- **Kharak Singh Case, 1962:** It was the first instance where the **Supreme Court of India granted relief based on the Right to Privacy**, though it did **not formally recognize it as a fundamental right** at the time.
- **A.P. Shah Committee 2011:** It recommended comprehensive **privacy legislation**, proposing a unified law to protect **privacy** and **personal data** in both **private and public sectors.**
- **B.N. Srikrishna Committee 2017:** It recommended stronger **privacy laws** in India, including **data processing restrictions**, a **Data Protection Authority**, the **right to be forgotten**, and **data localization.**
- **Justice K S Puttaswamy (Retd) vs Union of India Case, 2017:** The Supreme Court unanimously affirmed that the **right to privacy** is a **fundamental right** inherent to life and liberty under **Article 21.**

Global Practices on Data Governance

- **European Union(EU):** The EU's **General Data Protection Regulation (GDPR)** is a **comprehensive law protecting personal data**, recognizing privacy as a **fundamental right** that safeguards individual dignity and control over personal information
- **China:** The **Data Security Law (DSL)** mandates **classifying business data** by importance and imposes **new restrictions on cross-border data transfers**.
    - The **Personal Information Protection Law (PIPL)** grants Chinese data principals new rights to prevent the misuse of personal data.
- **United States:** The US lacks a **comprehensive privacy law** like the EU's GDPR, relying instead on **sector-specific regulations**. Government data use is governed by broad laws like the **Privacy Act**, while the private sector follows limited, sector-specific rules.

Conclusion

The **DPDP Act, 2023** establishes India's first **comprehensive data protection framework**, balancing **privacy rights** with **lawful data processing**. The 2025 Draft Rules enhance compliance, introduce **digital grievance redressal**, and permit **cross-border data flows**, aligning with global standards like the **EU's GDPR** while addressing local needs.

Drishti Mains Question:

Discuss the significance of the Digital Personal Data Protection Act, 2023 in safeguarding the fundamental right to privacy under Article 21.

UPSC Civil Services Examination, Previous Year Question (PYQ)

Prelims

Q. '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)

Q. 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)

Q. Describe the context and salient features of Digital Personal Data Protection Act 2023.(2024)

PDF Refernece URL: https://www.drishtiias.com/printpdf/dpdp-act-2023-and-dpdp-rules-2025