DIGITAL PERSONAL DATA PROTECTION ACT - POLITY

News: NITI Aayog, the top think tank of the government, had opposed some of the provisions of the Digital Personal Data Protection Act 2023.

WHAT'S IN THE NEWS?

NITI Aayog's Concerns Over the DPDP Bill

- The **DPDP Bill** suggested an amendment to **Section 8(1)(j)** of the **RTI Act**, which would restrict the disclosure of personal information related to public officials, even if there is a **larger public interest** at stake.
- During **inter-ministerial consultations**, **NITI Aayog** advised the **Ministry of Electronics and Information Technology (MeitY)** not to proceed with the bill in its current form, warning that it could potentially **weaken the RTI Act**.
- **Opposition parties** and **civil society activists** also voiced their objections to the amendment during the consultation period, and later when the bill was debated in Parliament.
- Despite these reservations, the **MeitY** did not make changes to the **RTI Act** in the proposed amendment.
- The government defended the changes, arguing that the **right to privacy** is a **fundamental right** under the **Indian Constitution**, which should also be extended to **government officers**.

Salient Features of the Digital Personal Data Protection Act (DPDPA) 2023

Empowerment of Individuals:

- Grants individuals rights to access, correct, and erase their personal data.
- Provides citizens with enhanced control over their personal information.

Consent Requirement:

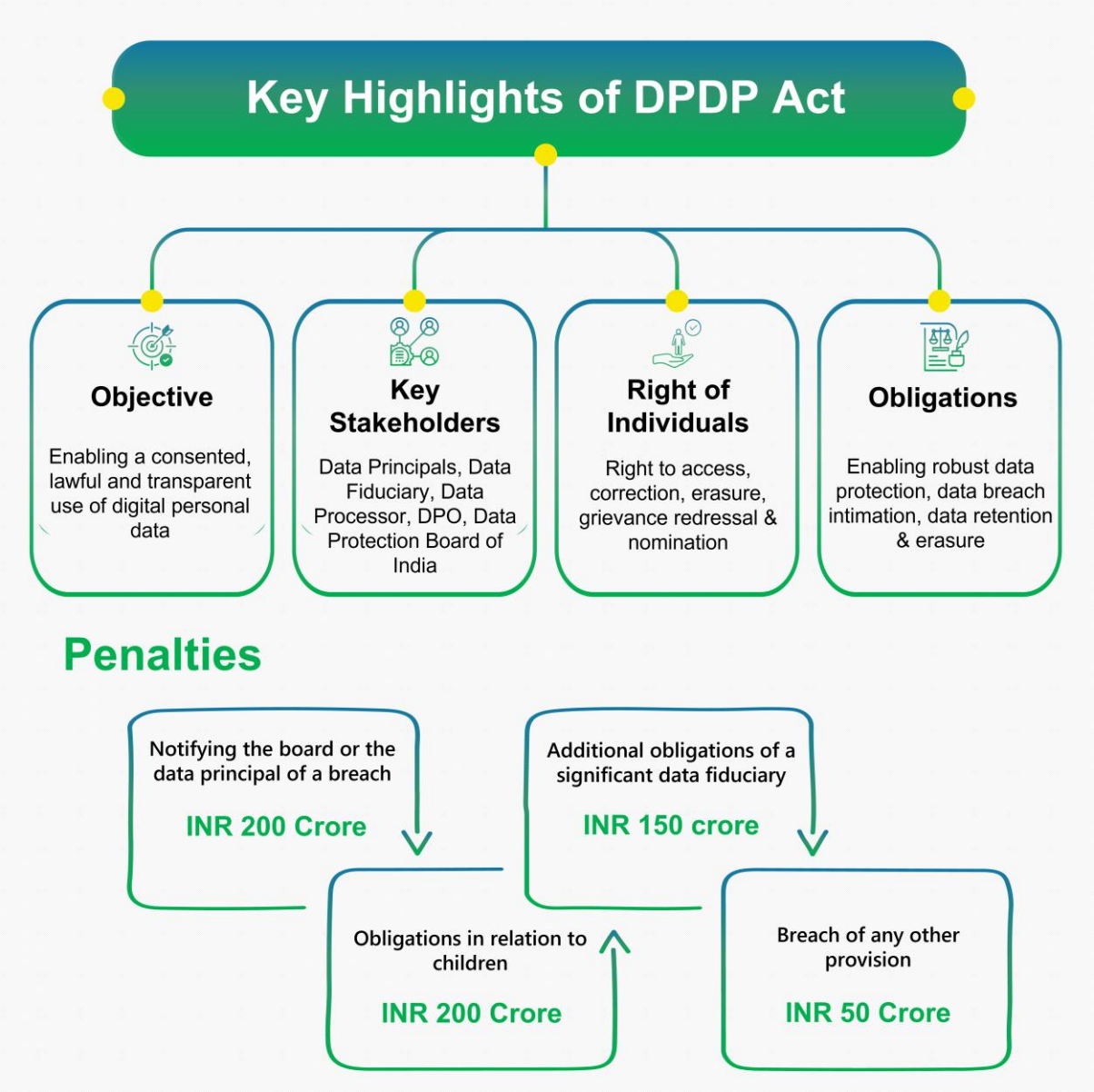
- Stipulates that personal data can only be processed with explicit consent from individuals.
- Organizations must present clear and specific consent forms and secure consent before collecting data.

Data Localization:

- Mandates that certain sensitive personal data must be stored and processed within India.
- Aims to bolster data security and simplify the enforcement of data protection regulations.

Establishment of Data Protection Board:

- Creates the Data Protection Board of India (DPBI) to oversee compliance and address grievances.
- The Board is tasked with resolving disputes and imposing penalties for non-compliance.



Breach Notification:

- Requires organizations to inform both individuals and the Data Protection Board about any data breaches that could compromise personal information.
- Promotes transparency and prompt action in the event of data leaks.

Penalties for Non-Compliance:

- Imposes substantial fines for violations to encourage adherence to data protection standards.

Issues with Obtaining Parental Consent

Consent Requirement for Children's Data:

- Section 9 of the DPDPA mandates that data fiduciaries must obtain verifiable consent from parents or guardians before processing children's data.
- Prohibits harmful data processing and ad targeting aimed at minors.

Exemptions:

- Certain entities, such as healthcare and educational institutions, may be exempt from obtaining verifiable parental consent under specific conditions.
- Limited exemptions are allowed based on the particular purpose for which the child's data is processed.

Challenges in Implementation:

- Difficulties in age verification and defining harm to children remain significant.
- Issues arise when parents revoke consent or when children reach the age of consent.
- Storing biometric data and ensuring compatibility across devices pose practical challenges.
- The act lacks clear guidance on how platforms should perform age-gating.

Delay in Rules Implementation:

- The delay in finalizing data protection rules is primarily due to unresolved issues regarding verifiable parental consent.
- The DPDPA requires at least 25 provisions to operationalize the act, adding to the complexity.

Proposed Solutions:

- The Ministry of Electronics and IT (MeitY) initially considered using the DigiLocker app, but privacy and scalability concerns led to its rejection.
- Another suggestion was an electronic token system, but it faced practical limitations.
- A recent industry meeting proposed a graded approach based on risk, with the UK's Age Appropriate Design Code (AADC) as a reference model.

Addressing the Issue of Parental Consent

Self-Declaration by Parents:

- Companies can allow parents to declare their relationship with the child during the account setup process.
- This method depends on the honesty of the parents and lacks a robust verification mechanism.

Two-Factor Authentication (2FA):

- Implementing 2FA for parental accounts can enhance security.
- Parents receive a verification code via SMS or email to confirm their consent, adding an extra layer of security.

Biometric Verification:

- Utilizing biometric methods, such as fingerprint or facial recognition, for parental consent can be both secure and privacy-conscious.
- Biometrics offer a high level of security by ensuring that only the authorized parent can provide consent.

Proxy Consent:

- Allowing parents to authorize a trusted third party, such as a school or pediatrician, to verify their relationship with the child.
- This approach can provide additional verification and ease the process of obtaining consent.

Source: https://indianexpress.com/article/india/govt-ignored-niti-red-flag-that-data-protection-law-could-weaken-rti-9593569/