Digital Personal Data Protection

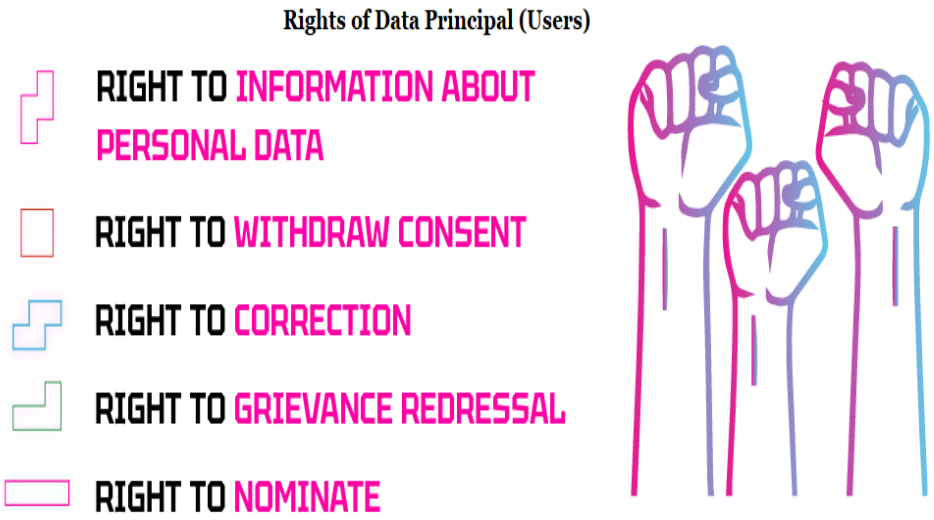
Why in News?

Recently the Union government notified the draft rules on Digital Personal Data Protection act,2023.

What are the key features of draft Digital Personal Data Protection Rules?

- **DPDP Rules** - These rules seek to operationalize the Digital Personal Data Protection Act, 2023 (DPDP Act), in line with India's commitment to create a robust framework for protecting digital personal data.
- **Aim** - To safeguard citizens' rights for the protection of their personal data.
- To Strengthen data protection regulations and foster trust between users and digital platforms.
- To Achieve the right balance between regulation and innovation.
- To Share benefits of India's growing innovation ecosystem to all citizens.
- **Applicability** – It is applicable to
    - E-commerce entities with at least 2 crore registered users in India.
    - Online gaming intermediaries with not less than 50 lakh registered users.
    - Social media intermediaries with at least 2 crore registered users.
- **Informed consent** - Data Fiduciary must provide the Data Principal(the user) the itemized list of personal data being collected and the purpose of collection.
- **Prior notification** - Data provider must send out a notice 48 hours in advance alerting the individual that it intends to erase his/her personal data from its servers.
- **Consent manager - A** company be incorporated in India as consent manger by the data fiduciary to enable users using its platform to give consent to the processing of their personal data.
- **Data rights** - Citizens are empowered with rights to demand data erasure, appoint digital nominees, and access user-friendly mechanisms to manage their data.
- **Withdrawal of consents** - Individual should be able to withdraw consent just as easily as it is given.
- **Data access by states** - The State agencies may process the personal data of users to provide or issue subsidies, benefits, services, certificates, licenses, or permits, as defined under law or policy or using public funds.
- **Security safeguards** - Data Fiduciary must implement reasonable security measures to protect personal data, including encryption, access control, monitoring for unauthorized access, and data backups etc.
- **Intimation of data breach** - Information about every data breach must be provided in 72 hours of that event.
- **Data Protection Officer (DPO)** - Every Data Fiduciary must clearly display on their website or app the contact details of a designated person who can address questions regarding the processing of personal data.

- **Parental consent** - Verifiable consent from parents or legal guardians must be obtained before processing the personal data of children or persons with disabilities.
- **Audit** - Fiduciaries must conduct a Data Protection Impact Assessment (DPIA) and a comprehensive audit once every year.
- **Rights of users** - Data Fiduciaries and Consent Managers must clearly publish on their website or app the process by which Data Principals can exercise their rights under the Act.



- **Data Protection Board** – It will function as a digital office, with a digital platform and app to enable citizens to approach it digitally and to have their complaints adjudicated without their physical presence being required.
- **Processing of personal data outside India**—Transferring Indian user's personal data outside is subject to the government restriction.

DPDP Act permits cross border transfer of data, apart from blacklisted jurisdictions.

What are the concerns with the rules?

- **Lack of clarity** - Proposed DPBI's institutional design have not been clearly spelt out.
- **Inadequate transparency** – Recommendations of the Justice B.N. Srikrishna committee convened to draft the first Bill for data protection, is not placed in public domain.
- **Ambiguous** - No explicit mechanism to ensure that the consent is sourced from the parent.
- **Retaining data** - Data fiduciaries are being permitted to retain data for up to three years from the last interaction or the date from which the rules come into effect.
- **Inadequate compliance mechanism** - Rules do not provide for a credible enforcement mechanism to ensure compliance of many provisions such as data breach notification, parental consent.
- **Cross-border processing of information** – It is not clear which countries will be permitted to access personal data of Indian consumers.

- **Challenges for businesses** - Maintaining consent artefacts and offering the option to withdraw consent for specific purposes could necessitate changes at the design and architecture level of applications and platforms.

What lies ahead?

- It must be ensured that minimising data collection, promoting disclosures, penalising neglect in protecting user data, and discouraging surveillance practices, both by the private sector and the government.
- Enhance operational clarity in certain areas such as parental consent, cross border data processing.
- Continued input and guidance from the government will be essential to drive effective implementation.

References

1. PIB | Draft Digital Personal Data Protection Rules
2. The TelegraphOnline | DPDP Rules