Balancing Privacy and Innovation

Posted at: 07/01/2025

Balancing Privacy and Innovation: Key Features of India's Digital Data Protection Rules

Context

The **Union Government of India** recently notified the **draft rules under the Digital Personal Data Protection (DPDP) Act, 2023**. These draft rules aim to operationalize the DPDP Act by establishing a comprehensive framework for protecting digital personal data. This step aligns with India's broader commitment to safeguarding the rights of its citizens in the digital age while fostering trust between users and digital platforms.

Key Features of the Draft Digital Personal Data Protection Rules

1. Objectives of the Rules

- **Aim:**
  - To **protect personal data** and uphold citizens' rights.
  - To **strengthen data protection regulations** while fostering innovation.
  - To ensure the **benefits of India's digital ecosystem** are accessible to all.

---

2. Applicability

The draft rules apply to:

- **E-commerce entities** with at least **2 crore registered users** in India.
- **Online gaming intermediaries** with **50 lakh or more registered users**.
- **Social media intermediaries** with a user base of **2 crore or more**.

---

3. Provisions and Safeguards

- **Informed Consent:**
  - Data Fiduciaries must provide an itemized list of personal data being collected and its intended purpose to the user (Data Principal).

- **Prior Notification:**
  - A **48-hour prior notice** is required before erasing personal data from servers.
- **Consent Manager:**
  - A **Consent Manager** registered in India must facilitate users in giving and managing consent for their data.
- **Data Rights for Users:**
  - Users are empowered to:
    - Demand **data erasure**.
    - Appoint **digital nominees**.
    - Access easy mechanisms to manage their data.
- **Withdrawal of Consent:**
  - Consent withdrawal must be as simple as granting consent.
- **State Access to Data:**
  - Government agencies can process personal data for public welfare programs like subsidies, benefits, or licenses.
- **Security Safeguards:**
  - Fiduciaries must implement measures such as **encryption**, **access control**, and **data backups** to protect user data.
- **Data Breach Notification:**
  - Breaches must be reported within **72 hours** of the event.
- **Parental Consent:**
  - Verifiable consent is required from parents or guardians for processing children's data.
- **Annual Audit:**
  - Fiduciaries must conduct a **Data Protection Impact Assessment (DPIA)** and a comprehensive audit annually.

---

4. Data Protection Board (DPB)

- Will function as a **digital platform**, enabling users to file complaints and resolve disputes online without physical presence.

---

5. Cross-Border Data Transfer

- **Permitted with restrictions:** Data can be transferred outside India, excluding blacklisted jurisdictions, subject to government oversight.

Concerns with the Draft Rules

1. Lack of Clarity

- The institutional framework for the **Data Protection Board of India (DPBI)** remains undefined.

2. Limited Transparency

- Recommendations from the **Justice B.N. Srikrishna Committee**, which drafted the first data protection bill, have not been disclosed.

3. Ambiguity in Provisions

- Parental consent mechanisms are not explicitly detailed.

4. Data Retention Issues

- Data Fiduciaries can retain user data for **up to three years** after the last interaction, raising privacy concerns.

5. Weak Compliance Mechanisms

- No robust mechanism to enforce provisions like data breach notifications or parental consent.

6. Cross-Border Data Processing

- Lack of clarity on which countries will be authorized to access Indian user data.

7. Challenges for Businesses

- Compliance with rules may require significant changes to application design and architecture, especially for managing consent artefacts and withdrawals.

The Way Forward

1. **Strengthen Privacy Practices:**
    - Minimise data collection.
    - Promote transparency in data handling.
    - Penalise negligence in protecting user data.
2. **Enhance Operational Clarity:**

- Provide clear guidelines on parental consent and cross-border data transfer.

3. **Empower Compliance Mechanisms:**
    - Introduce strong enforcement frameworks for timely reporting of breaches and ensuring user rights.
4. **Encourage Stakeholder Collaboration:**
    - Seek inputs from businesses, civil society, and data experts for effective rule implementation.
5. **Build Public Awareness:**
    - Educate citizens and businesses about their rights and responsibilities under the DPDP Act.

Conclusion

The **Draft Digital Personal Data Protection Rules, 2023**, represent a significant step in India's journey toward a secure digital environment. By addressing gaps in enforcement, operational clarity, and transparency, these rules can foster trust and innovation in India's digital economy.

A balanced approach—prioritising **citizen rights**, **data protection**, and **technological innovation**—will be crucial in ensuring the success of this transformative framework.