

Digital Personal Data Protection (DPDP) Rules 2025 - Operationalising India's Privacy Framework

December 3, 2025 • vajiramandravi.com



Digital Personal Data Protection (DPDP) Rules 2025 Latest News

- The Government of India has notified the Digital Personal Data Protection (DPDP) Rules 2025, **marking the complete operationalisation of the DPDP Act 2023.**
- This comes eight years after the Supreme Court's **K.S. Puttaswamy (2017) judgment** that declared privacy a fundamental right.
- The rules seek to **strengthen data protection, detail compliance mechanisms**, and define the roles of Data Fiduciaries, Data Principals, and the Data Protection Board of India (**DPBI**).

Key Features of the DPDP Act and Rules

- **Citizen-centric legal architecture:**
 - **SARAL (Simple, Accessible, Rational, and Actionable) design:** Uses plain language and illustrations for ease of compliance.

- **Rights and duties:**
 - **Data Principals (citizens):** Rights to consent, correction, erasure, grievance redressal.
 - **Data Fiduciaries (entities):** Obligations to process data lawfully, ensure security safeguards, and report breaches.
- **Phased implementation timeline:**
 - **Immediate provisions:**
 - **DPBI** operationalised with four members, headquartered in New Delhi.
 - Amendment to **Right to Information (RTI) Act** 2005 becomes effective, restricting disclosure of “personal information”.
 - **Delayed provisions (12-18 months):**
 - Informed consent requirements.
 - Purpose limitation in data processing.
 - Mandatory breach notification to users.
 - Appointment of Data Protection Officers (DPOs).
 - Launch of Consent Manager Framework (Nov 2026).
 - Full compliance for large tech firms (expected by May 2027).
- **Data Fiduciaries and Significant Data Fiduciaries (SDFs):**
 - **Categories:**
 - Determined by volume and sensitivity of data processed.
 - Criteria include impact on **sovereignty, democracy, national security, and public order**.
 - Major global and Indian tech companies (Meta, Google, Apple, Microsoft, Amazon) expected to be classified as **SDFs**.
 - **Obligations of SDFs:**
 - Higher compliance standards.
 - Data protection impact assessments.
 - Mandatory verification of **parental consent** for children’s data.
- **Data localisation and transfers:**
 - **Rules introduce conditional data localisation:**
 - The government will specify categories of personal and traffic data that cannot leave India.
 - To be decided by a government-appointed committee.
 - Significant pushback expected from global tech firms.
 - **Industry view:** Nasscom-Data Security Council of India (DSCI) stresses **interoperability-friendly cross-border frameworks**.
- **Processing of children’s data:**
 - Companies must adopt mechanisms for verifiable parental consent.
 - No government-prescribed model—flexibility given to firms.
 - **Behavioural tracking and targeted ads** for children generally prohibited, but limited processing allowed to prevent exposure to harmful content.
- **Breach notification and penalties:**
 - **Obligations:** Inform impacted users “without delay” regarding nature and extent of breach, timing and location, expected consequences, mitigation steps.

- **Penalties:** Up to ₹250 crore for failure to prevent data breaches. Wide powers vested in DPB to investigate and penalise.

Criticism of the Rules

- **Weakening the RTI Act:** For example, removal of public interest override for personal information of public officials reduces transparency.
- **Civil society concerns:** According to the Internet Freedom Foundation (IFF), rules enable extensive data collection by state agencies, and lack structural safeguards and oversight.
- **Wide government exemptions:** Concerns over “State and its instrumentalities” receiving broad exemptions **may undermine privacy protections and enable unchecked data processing** by state agencies.
- **Data localisation pushback:** Creates compliance burden on global tech companies; may affect India’s digital trade relations.
- **Delayed implementation:** Key citizen protections (consent, breach notification, erasure rights) postponed by 12–18 months.
- **Ambiguity in parental consent mechanisms:** Companies lack clarity on acceptable models; risk of inconsistent approaches.
- **Capacity constraints for DPBI:** Only four members could be insufficient for a country with massive digital penetration.
- **Compliance burden on small firms:** Rules may disproportionately affect startups with limited resources.

Way Forward

- **Strengthen independent oversight:** Ensure DPBI functions autonomously with adequate staffing and resources.
- **Clarify data localisation norms:** Engage with industry and global partners to build interoperable transfer mechanisms.
- **Restore transparency balance:** Re-examine RTI-related amendments to protect citizens’ right to information.
- **Provide transitional support to firms:** Standard templates and guidance for parental consent, breach notification, and consent management.
- **Build public awareness:** Large-scale digital literacy campaigns on data rights and responsibilities.
- **Enhance security standards:** Regular audits, incident response protocols, and minimum baseline cybersecurity norms.

Conclusion

- The DPDP Act 2023 and Rules 2025 **represent a landmark step** in India’s journey toward a modern, comprehensive data protection regime.
- They ensure **national security, public order, friendly relations** with foreign states, and aim to create an “**innovation-friendly**” ecosystem.

- While they fulfil **long-standing constitutional and policy commitments** to individual privacy, balancing privacy, transparency, innovation, and national security remains the central challenge.
- Effective implementation, **stakeholder consultation, and a robust oversight mechanism** will be critical to realising the full potential of India's digital privacy law.

Source: TH | IE

Source: <https://vajiramandravi.com/current-affairs/digital-personal-data-protection-dpdp-rules-2025-operationalising-indias-privacy-framework/>

© Vajiram & Ravi. For personal use only.