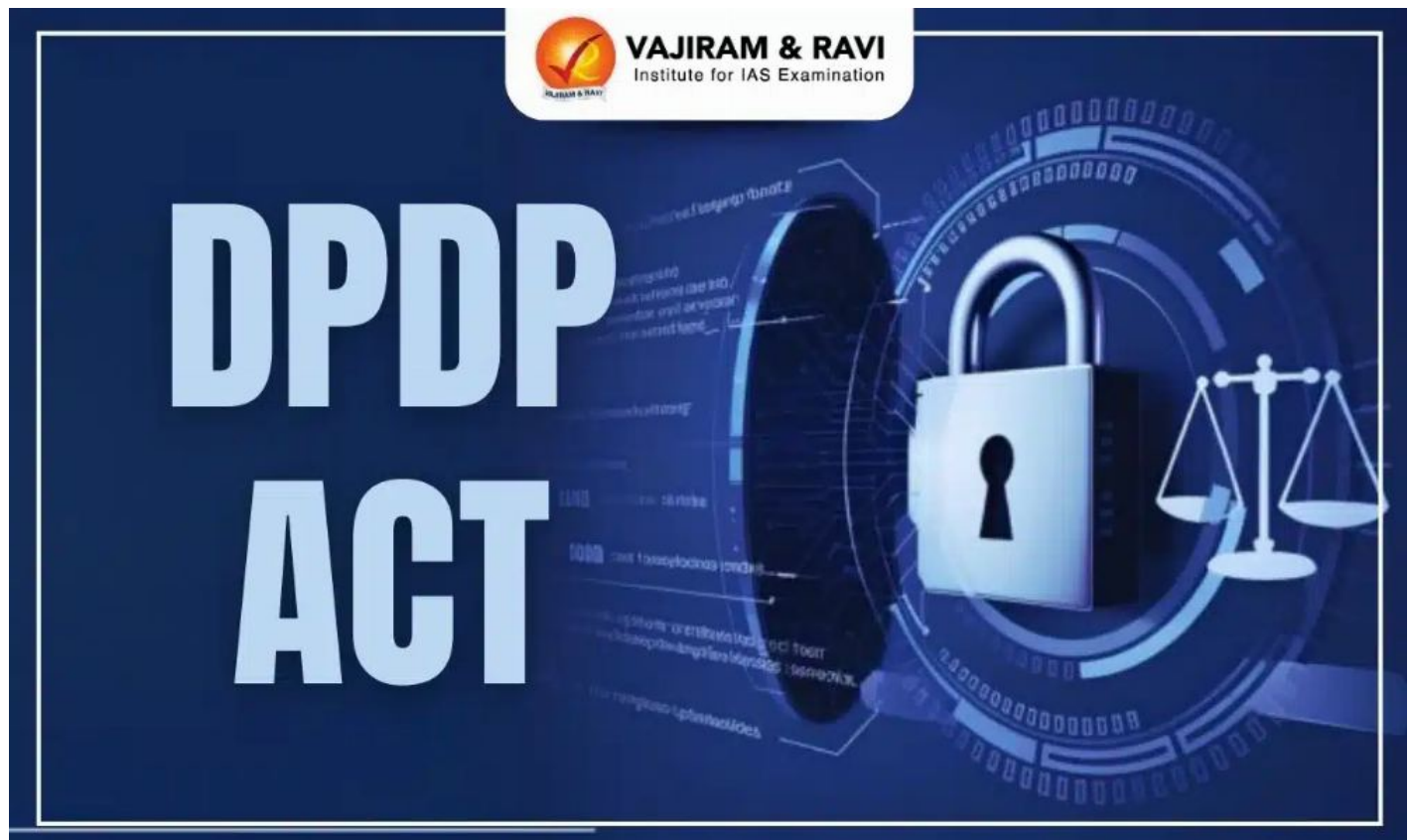


DPDP Act 2023, DPDP Rules 2025, Objectives, Provisions

November 26, 2025 • vajiramandravi.com



The Government of India notified the Digital Personal Data Protection (DPDP) Rules, 2025 on 14 November 2025, completing the full operationalisation of the DPDP Act 2023. Together, the Act and the Rules establish a clear, citizen-centric framework for the responsible handling of digital personal data. They balance the protection of individual rights with the need for lawful and accountable data processing. The detailed article has been shared below.

Digital Personal Data Protection (DPDP) Act 2023

The Digital Personal Data Protection (DPDP) Act 2023, enacted in August 2023, establishes India's legal framework for safeguarding digital personal data. It outlines the responsibilities of organisations that process such data and adopts the **SARAL** approach: **Simple, Accessible, Rational, and Actionable**, to ensure the law remains easy to understand and implement. The framework also seeks to balance the individual **Right to Privacy under Article 21** of the Indian Constitution with transparency by aligning its provisions with the **Right to Information (RTI) Act, 2005**.

DPDP Act 2023 Objectives

The objective of the DPDP Act 2023 is to make sure that people's personal information is kept private and protected while, at the same time, allowing certain types of data to be processed (for example, legally, securely, and appropriately) by both government and business entities. The purpose of the DPDP Act 2023 has been shared below.

- **Safeguarding Individual Privacy:** Provides a legal framework to protect personal data, prevent misuse, and limit unauthorised access or surveillance.
- **Ensuring Responsible Data Processing:** Allows data processing only for lawful purposes with user consent, ensuring accuracy, security, and timely deletion.
- **Consent-Centric Data Governance:** Requires clear, informed consent with the option to withdraw anytime; mandates parental consent for minors and persons with disabilities.
- **Balancing Privacy with Digital Innovation:** Reduces compliance burden for startups and small entities while imposing stricter obligations on major data processors.
- **Secure Cross-Border Data Flow:** Permits international data transfers to government-approved countries, supporting global digital operations with safeguards.

Also Read: [Consumer Protection Act 1986](#)

DPDP Act 2023 Features

- Establishes a consent-based system where personal data can be processed only with clear, informed, and revocable consent of the individual.
- Introduces rights for individuals, including the right to access, correct, erase personal data, and the right to grievance redressal.
- Provides special protections for children's data by requiring parental consent and prohibiting harmful data-processing practices.
- Allows classification of certain entities as **Significant Data Fiduciaries**, imposing stricter obligations like data audits and impact assessments.
- Includes provisions for government-notified exemptions in the interest of national security, public order, and research.
- Permits cross-border data transfers to approved countries while ensuring adequate protection safeguards.
- Follows the SARAL principle to keep rules simple, clear, and easy to implement for individuals and organisations.

Justice BN Srikrishna Committee

The Justice BN Srikrishna Committee was set up to study global data protection practices and recommend a comprehensive framework for India, which laid the groundwork for the initial draft of the DPDP Act.

The DPDP Act 2023 and subsequent DPDP Rules 2025 were finalised through public consultations and parliamentary enactment. The Ministry of Electronics and Information Technology carried forward the Committee's

recommendations to create India's citizen-centric data protection framework.

DPDP Act 2023 Provisions

The DPDP Act 2023 lays down a comprehensive legal framework for processing digital personal data in a lawful, transparent, and accountable manner. It outlines the rights of individuals, obligations of organisations, rules for consent, and a graded system of penalties for violations.

- The Act permits cross-border transfer of personal data to countries approved by the government, ensuring controlled and secure data flow.
- Personal data may be retained for up to three years from the last interaction, with mandatory 48-hour prior notice to the Data Principal before erasure.
- A digital-first **Data Protection Board of India (DPBI)** is established to handle consent, grievances, and enforcement through an online system for faster resolution.
- Major digital platforms with large user bases, such as social media and e-commerce giants, are designated as Significant Data Fiduciaries with enhanced obligations.
- The DPDP Act 2023 prescribes stringent monetary penalties for breaches by Data Fiduciaries. The maximum fine of **up to ₹250 crore** is imposed for failing to implement adequate security safeguards.
- Penalties of **up to ₹200 crore** may apply for not reporting a data breach or violating obligations related to children's data. For all other forms of non-compliance with the Act or its Rules, fines can go **up to ₹50 crore**.

Data Protection Board of India

A central pillar of the DPDP Act 2023 is the creation of the Data Protection Board of India, a dedicated authority to regulate compliance and address grievances.

Structure and Appointment

- Members are appointed by the Central Government.
- Tenure is two years, with eligibility for reappointment.

Data Protection Board of India (DPBI) Functions

- Enforcing compliance with the DPDP Act 2023.
- Monitoring and responding to data breaches.
- Investigating complaints and imposing penalties.
- Coordinating with organisations during breach incidents.
- Providing an online, digital-first grievance mechanism.
- Facilitating appeals to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

DPDP Rules 2025

The DPDP Rules 2025 provide detailed procedures, compliance timelines, and mechanisms to implement the DPDP Act 2023 effectively. They ensure citizen rights, secure data handling, and transparent grievance redressal while guiding organisations on responsible digital data management.

- DPDP Rules 2025 strengthen citizen rights, ensure responsible data use by organisations and curb unauthorised use of personal data.
- The Digital Personal Data Protection Rule reduces digital harms, supports innovation and helps build a secure, trusted digital economy for India.
- The DPDP framework puts citizens at the centre of data protection, giving them clear control over how their personal data is used.

Also Read: [Protection of Human Rights Act 1993](#)

How the DPDP Rules 2025 Empower Individuals

The DPDP framework strengthens citizen-centric privacy by giving individuals full control over how their personal data is collected, used, and protected. It ensures clear rights, transparent processes, and strict accountability for all Data Fiduciaries.

- **Right to Give or Refuse Consent:** Individuals can allow, deny, or withdraw consent anytime, and it must always be clear and informed.
- **Right to Know How Data Is Used:** Citizens may seek simple, clear information on what data is collected and why.
- **Right to Access Personal Data:** Individuals can request a copy of their personal data held by any Data Fiduciary.
- **Right to Correct or Update Data:** People may ask for corrections or updates when data is inaccurate or outdated.
- **Right to Erasure:** Personal data can be requested for deletion, and the Data Fiduciary must act within the allowed timeframe.
- **Right to Nominate Another Person:** Individuals can appoint someone to exercise their data rights on their behalf.
- **Mandatory 90-Day Response:** All requests for access, correction, updating, or deletion must be resolved within 90 days.
- **Breach Notification:** Individuals must be informed promptly with clear details if their data is compromised.
- **Contact Point for Queries:** Every Data Fiduciary must provide an accessible officer or DPO for grievance and query handling.
- **Protection for Children:** Processing children's data requires verifiable parental/guardian consent except for essential services.
- **Protection for Persons with Disabilities:** Consent must come from a verified lawful guardian when the individual cannot decide independently.

Challenges and Criticisms of the DPDP Act 2023

The DPDP Act 2023 faces several concerns regarding its implementation, enforcement, and impact on individual privacy. Many experts argue that certain provisions may dilute accountability and grant excessive powers to the government.

- The Act grants wide exemptions to government bodies, which can weaken transparency and reduce accountability in how citizens' data is handled.
- It gives the government broad authority to access, process, or block data, creating concerns about potential overreach and surveillance.
- The absence of a fully independent regulatory authority limits neutral oversight and may affect fair enforcement of data protection rules.
- Some key terms remain loosely defined, leading to confusion among organizations about proper compliance and interpretation of obligations.
- The Act places minimal restrictions on cross-border data transfers, raising questions about data security and exposure to foreign laws.

Way Forward

- **Strengthen Independent Oversight:** Establish a more autonomous regulatory body to enhance public trust. For example, creating an independent Privacy Commission similar to the UK's ICO can ensure impartial supervision.
- **Improve Citizen Awareness:** Launch large-scale digital literacy campaigns on consent, data rights, and grievance mechanisms. Like the RBI's "RBI Kehta Hai" campaign, a nationwide "Data Suraksha" campaign could educate citizens.
- **Streamline Compliance for Startups:** Provide toolkits, model privacy policies, and simplified reporting formats for smaller firms. For instance, a government-issued "Startup Compliance Sandbox" could reduce operational burden.
- **Enhance Data Security Standards:** Mandate periodic security audits and certifications for high-risk platforms. A system akin to ISO 27001 certification could be adapted as an Indian standard for digital platforms.
- **Promote Privacy-by-Design Innovation:** Encourage companies to embed privacy features in new technologies. For example, apps could use automatic data minimisation or end-to-end encryption by default.

Source: <https://vajiramandravi.com/current-affairs/dpdp-act-2023/>

© Vajiram & Ravi. For personal use only.