BACKGROUNDERS
Press Information Bureau
Government of India

DPDP Rules, 2025 Notified

A Citizen-Centric Framework for Privacy Protection and Responsible Data Use

November 17, 2025

Key Takeaways

- **DPDP Rules notified** on 14 November 2025 after nationwide consultations.
- Consultation process received **6,915 inputs** shaping the final Rules.
- Rules give **full effect** to the Digital Personal Data Protection Act, 2023.

Introduction

The Government of India notified the **Digital Personal Data Protection (DPDP) Rules, 2025** on 14 November 2025. This marks the full operationalisation of the **Digital Personal Data Protection Act, 2023 (DPDP Act**). Together, the Act and the Rules form a clear and citizen-centred framework for the responsible use of digital personal data. They place equal weight on individual rights and lawful data processing.

The Ministry of Electronics and Information Technology invited public comments on the draft Rules before finalising them. Consultations were held in Delhi, Mumbai, Guwahati, Kolkata, Hyderabad, Bengaluru and Chennai. A wide range of participants took part in these discussions. Startups, MSMEs, industry bodies, civil society groups and government departments all offered detailed suggestions. Citizens also shared their views. In total, 6,915 inputs were received during the consultation process. These contributions played a key role in shaping the final Rules.[1]

With the notification of the Rules, India now has a practical and innovation-friendly system for data protection. It supports ease of understanding, encourages compliance and strengthens trust in the country's growing digital ecosystem.

Understanding the Digital Personal Data Protection Act, 2023

Parliament enacted the Digital Personal Data Protection Act on 11 August 2023. The law creates a full framework for the protection of digital personal data in India. It explains what organisations must do when

[1] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2148944

they collect or use such data. The Act follows the SARAL approach. This means it is Simple, Accessible, Rational and Actionable. The text uses plain language and clear illustrations so that people and businesses can understand the rules without difficulty.

Key Terms Under the DPDP Act, 2023

- **Data Fiduciary:** An entity that decides why and how personal data is processed, either alone or with others.
- **Data Principal:** The individual to whom the personal data relates. In the case of a child, this includes a parent or lawful guardian. For a person with a disability who cannot act independently, this includes the lawful guardian acting on their behalf.
- **Data Processor:** Any entity that processes personal data on behalf of a Data Fiduciary.
- **Consent Manager:** An entity that provides a single, transparent and interoperable platform through which a Data Principal may give, manage, review or withdraw consent.
- **Appellate Tribunal:** The Telecom Disputes Settlement and Appellate Tribunal (TDSAT), which hears appeals against decisions of the Data Protection Board.

The law rests on seven core principles. These include consent and transparency, purpose limitation, data minimisation, accuracy, storage limitation, security safeguards and accountability. These principles guide every stage of data processing. They also ensure that personal data is used only for lawful and specific purposes.

A central feature of the Act is the creation of the **Data Protection Board of India.** The Board functions as an independent body that oversees compliance, inquires into breaches and ensures that corrective measures are taken. It plays a key role in enforcing the rights granted under the Act and maintaining trust in the system.

Penalties Under the DPDP Act, 2023

The DPDP Act imposes substantial financial penalties for non-compliance by Data Fiduciaries. The highest penalty up to **₹250 crore** applies to failure of a Data Fiduciary to maintain reasonable security safeguards. Not notifying the Board or affected individuals of a personal data breach as well as violations of obligations relating to children can each attract penalties of up to **₹200 crore**. Any other violation of the Act or Rules by a Data Fiduciary may attract penalties up to ₹50 crore.

The Act places clear responsibilities on Data Fiduciaries to keep personal data safe and to stay accountable for its use. It also gives Data Principals the right to know how their data is handled and the right to seek correction or removal when needed.

Together, the Act and the Rules create a strong and balanced system. They strengthen privacy, build public trust and support responsible innovation. They also help India's digital economy grow in a secure and globally competitive way.

Overview of the Digital Personal Data Protection Rules, 2025

The Digital Personal Data Protection Rules, 2025 give full effect to the DPDP Act, 2023. They build a clear and practical system to protect personal data in a fast-expanding digital environment. The Rules focus on the rights of citizens and on responsible data use by organisations. The Rules aim to curb unauthorized commercial use of data, reduce digital harms and create a safe space for innovation. They will also help India maintain a strong and trusted digital economy.

In carrying this vision forward, the Rules outline several core provisions that follow:

Phased and Practical Implementation

The Rules introduce an eighteen-month period for phased compliance. This gives organisations enough time to adjust their systems and adopt responsible data practices. Every Data Fiduciary must issue a separate consent notice that is clear and easy to understand. The notice must explain the specific purpose for which personal data is collected and used. Consent Managers, who help people manage their permissions, must be companies based in India.

Clear Protocols for Personal Data Breach Notification

The Rules set out a simple and timely process for reporting personal data breaches. When a breach takes place, the Data Fiduciary must inform all affected individuals without delay. The message must be in plain language and must explain what happened, the possible impact and the steps taken to address the issue. It must also include contact details for help.

Transparency and Accountability Measures

The Rules require every Data Fiduciary to display clear contact information for queries related to personal data. This may be the contact of a designated officer or a Data Protection Officer. Significant Data Fiduciaries face stronger duties. They must conduct independent audits and carry out impact assessments.

They must also follow stricter checks while using new or sensitive technologies. In some cases, they must follow government directions on restricted categories of data, including local storage where needed.

Strengthening Rights of Data Principals

The Rules reinforce the rights already provided under the Act. Individuals can ask to access their personal data or seek corrections and updates. They may also request the removal of data in certain situations. They can choose someone else to exercise these rights on their behalf. Data Fiduciaries must respond to such requests within ninety days.

Digital-First Data Protection Board

The Rules establish a fully digital Data Protection Board of India, which will consist of four members. Citizens will be able to file complaints online and track their cases through a dedicated portal and mobile application. This digital system supports quicker decisions and simplifies grievance redressal. Appeals against the Board's decisions will be heard by the Appellate Tribunal, TDSAT.

How the DPDP Rules Empower Individuals

The DPDP framework places the individual at the centre of India's data protection system. It aims to give every citizen clear control over personal data and confidence that it is being handled with care. The rules are written in plain language so that people can understand their rights without difficulty. They also ensure that organisations act responsibly and remain accountable for how they use personal data.

Rights and protections for citizens include:

Right to Give or Refuse Consent

Every person has the choice to allow or deny the use of their personal data. Consent must be clear, informed and easy to understand. Individuals may withdraw their consent at any time.

Right to Know How Data is Used

Citizens can seek information on what personal data has been collected, why it has been collected and how it is being used. Organisations must provide this information in a simple form.

Right to Access Personal Data

Individuals can ask for a copy of their personal data that is held by a Data Fiduciary.

Right to Correct Personal Data

People may request corrections to personal data that is inaccurate or incomplete.

Right to Update Personal Data

Citizens can ask for changes when their details have altered, such as a new address or updated contact number.

Right to Erase Personal Data

Individuals may request the removal of personal data in certain situations. The Data Fiduciary must consider and act on this request within the permitted time.

Right to Nominate Another Person

Every individual can appoint someone to exercise their data rights on their behalf. This is helpful in cases of illness or other limitations.

Mandatory Response within Ninety Days

Data Fiduciaries are required to address all requests related to access, correction, updating or erasure within a maximum of ninety days, ensuring timely action and accountability.

Protection During Personal Data Breaches

If a breach takes place, citizens must be informed at the earliest. The message must explain what happened and what steps they can take. This helps people act quickly to reduce harm.

Clear Contact for Queries and Complaints

Data Fiduciaries must provide a point of contact for questions relating to personal data. This may be a designated officer or a Data Protection Officer.

Special Protection for Children

When a child's personal data is involved, verifiable consent from a parent or guardian is required. This consent is needed unless the processing relates to essential services such as healthcare, education or real-time safety.

Special Protection for Persons with Disabilities

If a person with a disability cannot make legal decisions even with support, their lawful guardian must give consent. This guardian must be verified under the relevant laws.

How DPDP Aligns with the RTI Act[2]

Since the DPDP Act and the DPDP Rules expand citizens' privacy rights, they also clarify how these rights work alongside the access to information guaranteed by the Right to Information (RTI) Act.

The changes introduced through the DPDP Act revise Section 8(1)(j) of the RTI Act in a way that respects both rights without diminishing either. The amendment reflects the Supreme Court's affirmation of privacy as a fundamental right in the Puttaswamy judgment. It brings the law in line with the reasoning already followed by courts, which have long applied reasonable restrictions to safeguard personal information. By codifying this approach, the amendment prevents uncertainty and avoids any conflict between the transparency regime of the RTI Act and the privacy safeguards introduced under the DPDP framework.

The revision does not prevent the disclosure of personal information. It simply requires that such information be assessed with care and shared only after considering the privacy interests involved. At the same time, Section 8(2) of the RTI Act remains fully operative. This provision allows a public authority to release information when the public interest in disclosure is strong enough to outweigh any possible harm. This ensures that the essence of the RTI Act, which is to promote openness and accountability in public life, continues to guide decision making.

Conclusion

The Digital Personal Data Protection Act and the DPDP Rules mark an important step in building a trustworthy and future-ready digital environment for the country. They bring clarity to how personal data must be handled, strengthen the rights of individuals and create firm responsibilities for organisations. The framework is practical in design and backed by wide public consultation, which makes it both inclusive

[2] https://sansad.in/getFile/loksabhaquestions/annex/185/AS384_zFw7nl.pdf?source=pqals

and responsive to real needs. It supports the growth of India's digital economy while ensuring that privacy remains central to its progress. With these measures now in place, India moves towards a safer, more transparent and innovation-friendly data ecosystem that serves citizens and strengthens public confidence in digital governance.

References:

Full DPDP Rules, 2025:

- https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf

Full DPDP Act, 2023

- https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

MEITY:

- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014
- https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/jan/doc202515481101.pdf
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2090271
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2148944
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2158506

SA