

Digital Personal Data Protection Rules 2025

Posted at: 15/01/2025

Digital Personal Data Protection Rules 2025

The **Digital Personal Data Protection Rules 2025** have been introduced to complement the **Digital Personal Data Protection Act, 2023 (DPDP Act)**, which received **presidential approval** on **11th August 2023**. These rules lay out the necessary steps and framework for implementing the DPDP Act. Their main goal is to protect individuals' personal data and ensure that organizations handle it **fairly**, **transparently**, and **legally**. Below is a simplified breakdown of the key points and features.

Key Features of the Digital Personal Data Protection Act, 2023:

- 1. **Fairness**: Organizations must handle personal data in a way that is both **fair** and **transparent** to individuals.
- 2. Consent: Personal data can only be used after the individual gives clear and informed consent.
- 3. **Data Protection**: Individuals have the **right to know** how their data is being used and can request corrections or **removal** of it.

Components of Digital Data Protection:

1. Data Principal:

 This is the individual whose data is being processed. For children, their parents or guardians are the data principals. For people with disabilities, their legal guardians hold this role.

2. Data Fiduciaries:

 These are organizations or entities responsible for determining how and why personal data is processed. They must also ensure data is accurate, secure, and deleted when no longer needed.

3. Data Protection Board:

 $\circ\,$ This body ensures that organizations follow the rules. It can resolve complaints and

Key Features of the Draft Digital Personal Data Protection Rules 2025:

1. Notice to Data Principal:

- Data Fiduciaries must inform Data Principals with clear notices, detailing:
 - The **type** of data being processed.
 - The **purpose** of data processing.
 - How individuals can withdraw consent or file complaints.

2. Consent Management:

- Data Fiduciaries must get explicit consent before processing data and allow individuals to withdraw consent at any time.
- Consent Managers will help manage this process.

3. Obligations of Data Fiduciaries:

- Significant Data Fiduciaries (large organizations) have extra obligations like:
 - Annual audits and assessments.
 - Ensuring algorithms don't harm the rights of individuals.
 - Restricting some personal data transfers outside of India.
- General Obligations: Ensure transparency and provide grievance redressal systems.

4. Rights of Data Principals.

- Access and Erasure: Individuals can access their data or request it be erased.
- **Grievance Redressal:** Data Fiduciaries must address complaints within a specified time.
- **Nomination:** In cases of incapacity or death, individuals can nominate someone to act on their behalf.

5. Processing of Data Outside India:

Transferring data abroad is subject to specific government requirements.

6. Security Safeguards:

 Data Fiduciaries must use security measures like encryption, access control, and monitoring to protect data.

7. Personal Data Breach Intimation:

• If there is a breach, Data Fiduciaries must notify affected individuals within **48 hours** and report it to the Data Protection Board within **72 hours**.

8. Consent for Children's Data:

 Organizations must get parental or guardian consent before processing data of children.

9. Government Powers:

• The government can request data for specific purposes but must get prior approval before disclosing sensitive data.

Advantages of the Digital Personal Data Protection Rules 2025:

The rules create a "LIGHT BUT TIGHT" framework offering several benefits:

- Legal Certainty: Clear laws reduce confusion for businesses and individuals.
- Increased Trust: Builds confidence by ensuring privacy and security of data.
- Global Competitiveness: Aligns with international standards, helping Indian businesses compete globally.
- Harmonized Approach: Creates consistent rules across sectors.
- Technological Innovation: Encourages the development of privacy-enhancing technologies.
- User Empowerment: Gives individuals control over their personal data.
- Trustworthy Ecosystems: Promotes responsible and ethical data usage.

Challenges with the Framework:

Though the framework is strong, some challenges remain:

- 1. New Technologies: Emerging technologies like AI and IoT can be hard to regulate, especially in terms of bias and misuse.
- 2. **Technological Limitations:** Existing technologies may struggle to secure data from **cyber** threats.
- 3. **Social Impact: Issues like** the **digital divide** and potential misuse for **social surveillance** need to be addressed.
- 4. Operational Challenges: Organizations may face difficulties in implementing these rules.
- 5. **International Cooperation**: Data protection must be coordinated across borders, which can be complex.

Way Forward:

To ensure the rules are effective, the following steps should be taken:

- 1. **Awareness & Education**: Continually educate the public and organizations about data protection rights.
- 2. **Data Protection Impact Assessments (DPIAs)**: Encourage organizations to assess privacy risks proactively.
- 3. **Enforcement & Compliance**: Strengthen the **investigative** powers of the **Data Protection Board** and enforce penalties for non-compliance.
- 4. Quality Assurance: Regular audits and certifications will help ensure data protection

- standards are met.
- 5. User-Centric Approach: Focus on empowering individuals to control their data.
- 6. **Adaptability**: The framework should be flexible and updated regularly to meet emerging challenges.
- 7. **Technological Advancements**: Leverage technologies like **differential privacy** to enhance data protection.
- 8. Continuous Evaluation: Regularly assess the effectiveness of the Act and its rules.

Conclusion:

The **Digital Personal Data Protection Rules 2025** provide a strong foundation for protecting personal data in India. While there are some challenges, such as adapting to new technologies and coordinating international data policies, the rules offer a path forward for creating a **secure**, **trustworthy**, and **innovative** digital environment. By continuously updating and adapting the framework, India can strengthen its data protection system, benefiting both businesses and individuals alike.

