



CIVIL

Verifiable Consent for Processing Personal Data of Children and Persons with Disabilities Under Rule 10 of the proposed DPDP Rules, 2025

AUTHOR Rahul Sundaram

PUBLISHED 10 January 2025

In the changing environment of digital privacy, the proposed **Digital Personal Data Protection (DPDP) Rules, 2025**, lays emphasis on the importance of safeguarding personal data, particularly for vulnerable groups such as children and persons with disabilities. Rule 10 of these rules provides explicit guidance on obtaining **verifiable consent** for processing the personal data of these groups, ensuring their rights and privacy are adequately protected.

Table of contents

- [Key Provisions of Rule 10](#)
- [What Constitutes Verifiable Consent?](#)
- [Challenges in Implementing Verifiable Consent](#)
- [Best Practices for Compliance](#)
- [Conclusion](#)

Key Provisions of Rule 10

Rule 10 of the DPDP Rules establishes that:

1. **Children’s Personal Data:** For individuals under the age of 18, the consent required for processing their personal data must be obtained from their lawful guardian.
2. **Persons with Disabilities:** Where a person with disabilities has a lawful guardian, the guardian’s consent must be obtained for processing the individual’s personal data.
3. **Verifiability:** The consent must be verifiable, meaning that organizations collecting and processing the data must ensure the authenticity of the consent provided.

What Constitutes Verifiable Consent?

The concept of verifiable consent under Rule 10 implies that the consent mechanism must satisfy the following conditions:

- **Informed Consent:** The guardian must be fully aware of what data is being collected, the purpose of processing, and any associated risks.
- **Explicit and Affirmative Action:** The guardian must take a clear and affirmative action to provide consent, such as signing a document, checking a box, or using an OTP-based system.
- **Traceability:** The consent process must generate evidence that can be retained and audited to demonstrate compliance.
- **Granularity:** Consent should be specific to the data processing activity, avoiding blanket or vague permissions.

A Data Fiduciary, while obtaining verifiable consent from an individual identifying herself as the lawful guardian of a person with disability, shall observe due diligence to verify that such guardian is appointed by a court of law, a designated authority or a local level committee, under the law applicable to guardianship.

Challenges in Implementing Verifiable Consent

While Rule 10 sets out clear guidelines, its implementation may present challenges:

1. **Digital Literacy:** Guardians may lack the necessary literacy / digital literacy to comprehend the implications of consent, particularly in rural or underserved areas.
2. **Verification Mechanisms:** Developing strong and foolproof systems to verify the identity of lawful guardians and ensure their consent can be resource-intensive.
3. **Balancing Innovation and Compliance:** Businesses must navigate the fine line between innovation in data-driven services and strict adherence to data protection laws.

Best Practices for Compliance

To ensure compliance with Rule 10, data fiduciaries (entities processing personal data) should adopt the following best practices:

- **Use of Digital Tools:** Employ advanced verification technologies like Aadhaar-based authentication or secure biometric systems to ensure the identity of lawful guardians.

- **Comprehensive Documentation:** Maintain clear records of consent, including the guardian's authority and identity, the data being processed, and the purpose of processing.
- **Regular Audits:** Periodically audit consent processes to ensure compliance with legal standards and address any gaps.

Conclusion

Rule 10 of the proposed DPDP Rules, 2025, is a significant step toward enhancing the protection of personal data for children and persons with disabilities. By emphasizing verifiable consent and stringent safeguards, it strikes a balance between technological advancement and ethical responsibility. However, its success hinges on the commitment of data fiduciaries to uphold these standards and the proactive enforcement by regulatory authorities. In a world increasingly reliant on data, protecting the most vulnerable is a moral imperative, not just a legal obligation.

For further details write to contact@indialaw.in