DSCI Policy
policy@dsci.in

Frequently Asked Questions (FAQs) on the Processing of Personal Data of Children and Person with Disabilities

(Rules 10 & 11 of Data Protection Rules read with Section 9 of DPDPA)

I. General Scope and Implementation

Q1. When must an organisation comply with the new rules governing the personal data of children and persons with disabilities (Rules 10 and 11)?

The rules governing processing of children's data (Rule 10) and the verifiable consent for persons with disabilities (Rule 11), along with most operational rules (Rules 3, 5 to 16, 22, and 23), shall come into force **eighteen months (i.e. 12th May 2027)** after the date of publication of the Gazette.

Q2. How have the Final Rules restructured the protection requirements for children and persons with disabilities (PwD) compared to the Draft Rules?

The Final Rules separated the provisions:

1. Rule 10 now focuses exclusively on the Verifiable consent for processing of personal data of a child.
2. Rule 11 is dedicated entirely to Verifiable consent for processing of personal data of a person with disability who has a lawful guardian.

This structural re-organisation improves clarity, as the Draft Rules had combined both provisions under a single Rule 10 structure.

II. Processing Children's Personal Data (Rule 10)

Q3. What technical steps are mandatory for Data Fiduciaries (DFs) to ensure compliance when processing a child's data?

A Data Fiduciary is mandated to adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent is obtained before processing any personal data of a child. Additionally, the DF must exercise due diligence to verify that the individual identifying herself as the parent is an adult who is identifiable.

Q4. What are the permissible mechanisms for verifying parental identity and age?

The DF may reference identity and age verification by:

1. Reliable details of identity and age already available with the Data Fiduciary.
2. Voluntarily provided details of identity and age by the individual.
3. Details provided through a virtual token mapped to such identity and age details, provided this token is issued by an authorised entity.

Q5. Has the definition of an "Authorised Entity" been clarified or tightened compared to the draft stage?

Yes, the definition of "authorised entity" has been tightened in the Final Rules (Rule 10(2)(b)).

- Draft Rule Intent: An authorised entity was defined as one entrusted with the "maintenance" of identity and age details.
- Final Rule Intent: An authorised entity is defined as an entity entrusted with the "issuance" of details of identity and age or a virtual token mapped to such details.

This tightening means DFs must primarily rely on official or recognized bodies entrusted with the *issuance* function, potentially raising the bar for acceptable verification sources.

Q6. Can a Digital Locker service provider be used in the parental consent verification process?

Yes. The definition of "authorised entity" explicitly includes details of identity and age or tokens made available and verified by a Digital Locker Service Provider. Illustrations provided show that a parent (P) may **voluntarily** make such verification details available using the services of a Digital Locker Service Provider to verify that P is an identifiable adult.

III. Processing Data of Persons with Disabilities (Rule 11)

Q7. What is the specific due diligence requirement for verifying the lawful guardian of a Person with Disability (PwD)?

Rule 11(1) requires the Data Fiduciary to observe due diligence to verify that such guardian is appointed by a court of law, or by a designated authority or by a local level committee, under the law applicable to guardianship. This imposes a stringent requirement to confirm the legal standing of the guardian.

Q8. What acts define the “law applicable to guardianship” under Rule 11?

The "law applicable to guardianship" means the provisions of law contained in:

1. Rights of Persons with Disabilities Act, 2016 (for individuals with long-term physical, mental, intellectual, or sensory impairment who cannot take legally binding decisions despite adequate support).
2. National Trust Act, 1999 (for persons suffering from conditions like autism, cerebral palsy, mental retardation, or severe multiple disability who cannot take legally binding decisions).

IV. Exemptions (Fourth Schedule)

Q9. Which classes of Data Fiduciaries are generally exempted from obtaining consent (Section 9(1) and (3) of the Act) when processing a child's data, provided they meet conditions?

Part A of the Fourth Schedule exempts DFs operating in critical sectors, subject to specific conditions. These include:

- Clinical establishments, mental health establishments, or healthcare professionals: Processing must be restricted to the provision of health services to the extent necessary for the protection of the child's health.
- Educational institutions: Processing is restricted to tracking and behavioural monitoring for educational activities or in the interests of safety of children enrolled.
- Transport providers engaged by educational/childcare centres: Processing is restricted to tracking the location of such children, in the interests of their safety, during travel.

Q10. What specific processing purposes, beyond sector-specific exemptions, are permitted without full consent compliance for children?

Part B of the Fourth Schedule lists specific purposes that exempt DFs from Section 9(1) and (3) requirements:

1. Location Tracking (New Addition): Processing for the determination of real-time location of a child, restricted strictly to the tracking of real-time location in the interest of her safety and protection or security. This purpose was added in the Final Rules.
2. Age Confirmation: Processing necessary for the DF's due diligence to confirm that the Data Principal is not a child (observance of due diligence under Rule 10).
3. Welfare Benefits: Processing for providing or issuing any subsidy, benefit, service, certificate, licence, or permit under law or policy, or using public funds, in the interests of a child.
4. Harm Prevention: Processing for ensuring that any information, service, or advertisement likely to cause any detrimental effect on the well-being of a child is not accessible to her.