INDIA JURIS
International Law Firm

Children's Data and Verifiable Parental Consent

under India's DPDP Framework



Abstract

India's Digital Personal Data Protection Act, 2023 ("DPDP Act") treats children as a specially protected category of data principals. Section 9 requires a Data Fiduciary to obtain verifiable consent from a child's parent, or from the lawful guardian of a person with disability, before processing the child's personal data. The Digital Personal Data Protection Rules, 2025 ("DPDP Rules") operationalize this requirement through Rule 10, which prescribes technical and organizational measures for verifying that the person granting consent is an identifiable adult.

This paper examines the legal architecture governing children's personal data in India, the meaning and mechanics of verifiable parental consent, the prohibition on tracking, behavioral monitoring, and targeted advertising directed at children, and the limited exemptions carved out for essential services and child-safety purposes. It also evaluates the practical compliance challenges facing EdTech platforms, social-media companies, gaming services, healthcare providers, and other child-facing businesses. The paper argues that while the framework reflects a legitimate protective objective, its effectiveness will depend on proportionate age-assurance methods, clear guidance from the Data Protection Board, privacy-preserving verification technologies, and sector-specific implementation standards.

I. Introduction

Children are among the most active users of digital services, yet they are also among the least capable of understanding the long-term consequences of data collection, profiling, and online disclosure. Digital platforms collect information about children through account registrations, educational applications, gaming services, social media, connected devices, advertising technologies, and location-based services. Such data may be used to personalize content, recommend products, target advertisements, assess creditworthiness, or build behavioral profiles that follow a child into adulthood.

The DPDP Act recognizes this vulnerability. It creates a distinct regime for children's data, requiring parental consent and imposing restrictions on practices that can exploit children's attention, preferences, or online behavior. Section 9 of the DPDP Act is the central provision, while Rule 10 of the DPDP Rules supplies the operational detail for verifiable parental consent.

The policy question is not whether children require greater protection—there is broad consensus that they do—but how that protection can be implemented without excluding children from beneficial digital services, imposing excessive identity-collection burdens on families, or creating unworkable compliance obligations for smaller enterprises. This paper analyses that balance.

II.Statutory Framework

A. Who is a child?

Under Section 9 of the DPDP Act, a "child" is a person who has not completed eighteen years of age. The provision also extends protection to a person with disability who has a lawful guardian. In such cases, verifiable consent must be obtained from the lawful guardian before processing personal data.

This is a broad definition. Unlike some foreign regimes that apply heightened protections only to younger children, India applies the parental-consent requirement to all persons below eighteen. This has significant consequences for teenagers, particularly those using social media, online learning platforms, gaming services, and e-commerce platforms. A sixteen-year-old cannot independently provide valid consent for most processing of personal data; parental consent is required.[1]

B. The parental-consent mandate

Section 9(1) provides that a Data Fiduciary must, before processing any personal data of a child, obtain verifiable consent from the child's parent. Where the data principal is a person with disability having a lawful guardian, consent must be obtained from that guardian. The requirement applies before processing begins, not retrospectively.[2]

The word "verifiable" is crucial. The statute does not merely require a parent to click an "I agree" button. The Data Fiduciary must have reasonable technical and organizational measures to establish that the person consenting is an adult and is identifiable where required for legal compliance. This distinguishes parental consent from ordinary data-principal consent under the DPDP framework.[3]

C. Restrictions beyond consent

Parental consent does not authorize every form of processing. Section 9 imposes substantive restrictions irrespective of consent. A Data Fiduciary must not undertake tracking, behavioral monitoring, or targeted advertising directed at children. These restrictions are categorical and cannot be overcome merely because a parent has consented.

The Act also directs Data Fiduciaries to avoid processing that is likely to cause a detrimental effect on a child's well-being. This introduces a child-welfare standard into data processing, requiring businesses to assess not only legality but also the potential impact of their services on children.

---

[1] https://www.ey.com/en_in/insights/cybersecurity/india-s-data-privacy-shift-steering-the-dpdp-compliance-and- readiness

[2] https://www.pwc.in/assets/pdfs/digital-personal-data-protection-rules-2025.pdf

[3] https://www.dpdpa.com/DPDP_Rules_2025_English_only.pdf

III. Verifiable Parental Consent under Rule 10

A. Technical and organizational measures

Rule 10 of the DPDP Rules requires a Data Fiduciary to adopt appropriate technical and organizational measures to ensure that verifiable parental consent is obtained before processing a child's personal data. The Rule also requires due diligence to check that the individual identifying herself as the parent is an identifiable adult, where such identification is required for compliance with Indian law.

The Rule permits verification through:

- Reliable details of identity and age already available with the Data Fiduciary;
- Details of identity and age voluntarily provided by the individual; or
- A virtual token mapped to such details and issued by an authorized entity.

This structure gives businesses flexibility, but it also creates interpretative questions. What counts as "reliable" details already held by the Data Fiduciary? When is a virtual token appropriate? What level of assurance is sufficient for a low-risk educational application as opposed to a social-media platform with large-scale profiling risks?

B. Verification methods

The Rules do not mandate a single verification technology. Instead, they permit a risk-based approach using identity and age details, voluntary disclosures, or authorised virtual tokens. Commentary on the Rules suggests that verification may involve reliable identity and age information, voluntary provision of details, or virtual tokens issued by authorised entities.[4]

In practice, possible methods include:

- Document-based verification, where a parent submits government-issued identity or age proof;
- Knowledge-based verification, where the platform uses information already held about the parent;
- OTP or account-based verification, where the parent verifies control over a registered communication channel;
- Virtual tokens, where an authorised entity confirms adult status without disclosing the parent's full identity documents to the Data Fiduciary;
- Third-party age-assurance services, subject to appropriate contractual and security safeguards.

Each method carries trade-offs. Document verification may be accurate but creates a new cache of sensitive identity data. OTP verification is convenient but may not establish a parental relationship. Virtual tokens may reduce data exposure but require trusted intermediaries and interoperability standards.

[4] https://dpdp.lkslaw.com/provisions/childrens-data

C. The proportionality dilemma

The central design challenge is proportionality. If verification is too weak, children can bypass parental consent by falsely claiming to be adults or by using an adult's credentials. If verification is too intrusive, platforms may collect more personal data from parents than they collect from children, thereby undermining the privacy objective.

A proportionate framework should require stronger verification where the risks are higher—for example, social networking, advertising-driven platforms, or services involving public visibility, location data, or financial transactions. Lower-risk services, such as a basic homework application, should not be forced to collect government identity documents merely to allow a parent to approve an account.

The DPDP Rules appear to permit such differentiation by allowing reliance on details already available with the Data Fiduciary or voluntarily provided details, rather than prescribing a uniform identity-check requirement.

IV. Prohibited Practices

A. Tracking and behavioral monitoring

Section 9 prohibits tracking or behavioral monitoring of children. This is one of the most consequential provisions for digital businesses. It restricts the use of cookies, device identifiers, pixels, SDKs, and similar technologies to observe a child's online behavior for profiling or commercial purposes.

The prohibition is not limited to advertising. Behavioral monitoring may include analysing a child's browsing patterns, app usage, content preferences, social connections, or emotional responses to personalise services or build a profile. Even where a parent consents to processing of basic account information, the parent cannot authorise behavioural surveillance or targeted advertising.

B. Targeted advertising

The DPDP Act also prohibits targeted advertising directed at children. This means that a platform cannot use a child's personal data to serve advertisements selected on the basis of the child's interests, behaviour, location, or profile.

This does not necessarily prohibit all advertising to children. Contextual advertising—where an advertisement is displayed based on the content being viewed rather than the child's personal profile—may be less problematic. However, businesses must ensure that contextual advertising does not covertly rely on behavioural inference, device fingerprinting, or cross-site tracking.

C. Detrimental effect on well-being

The requirement to avoid processing likely to cause detrimental effects on a child's well-being is broader than the express prohibitions on tracking and targeted advertising. It may cover addictive design features, harmful content recommendations, excessive data collection, public disclosure

of sensitive information, or features that encourage children to share personal details.

This provision will likely require child-facing platforms to conduct child-impact assessments, review default privacy settings, limit data-sharing with third parties, and design age-appropriate interfaces. The emphasis shifts from formal consent to substantive protection.

V. Exemptions and Essential Services

A. Statutory exemptions

The DPDP framework recognises that a blanket parental-consent requirement could obstruct essential services. Section 9 permits the Central Government to exempt certain classes of Data Fiduciaries or processing activities where such exemption is necessary and in the interests of a child.

The DPDP Rules identify exemptions for certain entities and purposes, including clinical establishments, mental-health establishments, allied healthcare professionals, educational institutions, creches, child day-care centres, and transport entities providing services for children.

B. Child-safety purposes

The Rules also permit processing without parental consent in limited circumstances, including:

- Exercising a power, performing a function, or discharging a duty in the interest of a child under applicable law;
- Providing or issuing a subsidy, benefit, service, certificate, licence, or permit in the interest of a child;
- Creating a user account for email communication, limited to that use;
- Determining a child's real-time location in the interest of safety, protection, or security;
- Preventing access to information, services, or advertisements likely to harm a child's well-being.

These exemptions are purpose-limited. A healthcare provider may process a child's data to deliver medical care, but it cannot use that data for unrelated commercial profiling. An educational institution may process student data for educational administration, but it must not repurpose it for advertising or behavioural monitoring.

C. The boundary problem

The exemptions raise a boundary problem. For example, an EdTech platform may argue that it is an educational institution, while a gaming company may argue that certain features support child safety. The scope of these exemptions will therefore depend on the nature of the entity, the purpose of processing, and whether the processing is restricted to what is necessary.

Businesses should avoid treating exemptions as blanket licences. The safer approach is to document the exempted purpose, limit data collection to that purpose, and apply the same security, retention, and minimisation standards as would apply to consent-based processing.

VI. Compliance Challenges

A. Age assurance

The first practical challenge is determining whether a user is a child. Many platforms currently rely on self-declared age at registration. This is inadequate under the DPDP framework because a child can simply enter an adult birthdate.

At the same time, mandatory identity verification for every user would be disproportionate and privacy-invasive. Businesses may need to adopt layered approaches: neutral age-assurance signals at onboarding, heightened verification where child status is likely, and parental-consent flows where a user is identified as below eighteen.

B. Parental relationship

Verifying that a person is an adult is not the same as verifying that the person is the child's parent. The DPDP Rules emphasise verification that the consenting person is an identifiable adult, but the practical difficulty of confirming the parent-child relationship remains.

Strict relationship verification may require access to family records or government databases, raising privacy and exclusion concerns. A more practical approach may involve a combination of adult verification, account linkage, parental control features, and periodic confirmation, calibrated to the sensitivity of the processing.

C. Data minimisation

Parental-consent verification itself involves processing personal data. If a platform collects Aadhaar, identity documents, birthdates, phone numbers, or other details from parents, it must apply data-minimisation principles. The verification data should not be retained longer than necessary, should not be used for marketing, and should be protected with strong security controls.

Virtual tokens offer a promising solution because they can confirm adult status without transferring the parent's full identity documents to every platform. However, their success depends on the availability of authorised token issuers, interoperability, and user trust.

D. Third-party processors

Child-facing platforms often rely on cloud providers, analytics vendors, customer-support tools, payment processors, and advertising intermediaries. Each such processor may introduce additional data flows. Under the DPDP framework, the Data Fiduciary remains responsible for ensuring lawful processing.

Contracts with processors should expressly address children's data, prohibit behavioural profiling and targeted advertising, restrict sub-processing, require breach notification, and mandate deletion or de-identification upon termination.

E. Cross-border transfers

Many digital services operate across jurisdictions. Cross-border transfer of children's data may be permitted only to countries notified by the Central Government, subject to applicable sectoral restrictions. Businesses must map where children's data is stored, accessed, or processed, including by overseas support teams and cloud infrastructure.

VII. Sectoral Implications

A. EdTech

EdTech platforms are likely to be directly affected. They process student names, contact details, academic performance, attendance records, learning patterns, and sometimes biometric or location data. While educational institutions may benefit from exemptions for certain essential functions, commercial EdTech providers must carefully assess whether they fall within the exemption or require parental consent.

EdTech businesses should implement parent dashboards, clear notices, limited data retention, restrictions on third-party analytics, and child-safe recommendation systems.

B. Social media and gaming

Social-media and gaming platforms face the highest compliance burden. They typically rely on engagement metrics, recommendations, social graphs, and advertising revenue. The prohibition on behavioural monitoring and targeted advertising requires a fundamental redesign of child-facing experiences.

Platforms should provide age-appropriate defaults, disable behavioural profiling for identified child users, avoid public-by-default settings, and offer parental supervision tools without converting parental controls into surveillance tools.

C. Healthcare

Healthcare providers may process children's data for medical treatment under the exemption for essential services. However, they must still observe confidentiality, security, purpose limitation, and retention discipline. Telemedicine platforms, diagnostic laboratories, and health insurers should separate treatment-related processing from commercial analytics or marketing.pwc+1

D. E-commerce and fintech

E-commerce platforms and fintech companies must be cautious about profiling children for credit, loyalty, discounts, or financial products. The DPDP framework's restrictions on tracking and targeted advertising limit the use of children's data for commercial segmentation.

Recommendations

Businesses processing children's data should adopt the following measures:

1. **Conduct a children's-data inventory.** Identify all products, features, databases, vendors, and data flows involving users below eighteen.

2. **Implement age-appropriate onboarding.** Use proportionate age-assurance measures and route identified child users into parental-consent workflows.
3. **Design a verifiable consent journey.** Obtain consent before processing, record the consent artefact, identify the consenting adult through permitted verification methods, and allow withdrawal.
4. **Disable behavioural profiling for children.** Review cookies, SDKs, advertising identifiers, recommendation engines, and analytics tools to ensure that children are not tracked or profiled for targeted advertising.
5. **Apply privacy-by-default settings.** Restrict public visibility, limit data sharing, disable unnecessary personalisation, and avoid dark patterns that induce disclosure.
6. **Review vendor contracts.** Impose children's-data obligations on processors, including prohibitions on profiling, targeted advertising, and unauthorised sub-processing.
7. **Adopt retention limits.** Delete children's data when the purpose is served, the account is inactive, or retention is no longer necessary.
8. **Prepare breach-response protocols.** Ensure that breaches involving children's data trigger prompt assessment, containment, regulator notification, and communication with parents where appropriate.[5]
9. **Maintain accountability records.** Document the legal basis, verification method, consent records, exemptions relied upon, risk assessments, and vendor controls.

IX. Conclusion

The children's-data provisions of the DPDP Act and DPDP Rules represent a major shift in India's digital regulatory landscape. By requiring verifiable parental consent, prohibiting tracking and targeted advertising, and imposing a child-welfare standard, the framework seeks to protect children from exploitative data practices while preserving access to essential digital services.

The success of this regime will depend on implementation. Regulators must provide practical guidance on age assurance, verification standards, exemption boundaries, and permissible advertising models. Businesses must move beyond checkbox compliance and redesign products around data minimisation, child-safe defaults, and meaningful parental control. Parents, meanwhile, must be given tools that enable protection without normalising excessive surveillance of children.

[5] https://www.complydp.com/articles

Ultimately, verifiable parental consent should not be viewed as a mere regulatory formality. It is a governance mechanism through which families, businesses, and regulators share responsibility for ensuring that children can participate safely in the digital economy. A well-designed consent and age-assurance framework can protect children while supporting innovation, provided it remains proportionate, privacy-preserving, and practically enforceable.

About India Juris

India Juris is a full-service international law firm providing comprehensive legal solutions to a diverse range of clients, including corporates, financial institutions, and individuals. With a strong focus on delivering practical and result-oriented advice, the firm combines deep legal expertise with a clear understanding of business needs across sectors.

Follow us on :

www.indiajuris.com

Our Offices

New Delhi
Lajpat Nagar-1 New Delhi
newdelhi@indiajuris.com

Gurugram
Sohna Road, Gurugram
gurugram@indiajuris.com

Bengaluru
Indira Nagar, Bengaluru
bengaluru@indiajuris.com

Mumbai
Andheri East, Mumbai
mumbai@indiajuris.com

GIFT CITY, Gujarat
Processing Area GIFT SEZ, GIFT CITY
giftcity@indiajuris.com

In this document, India Juris refers to India Juris is a global consulting firm and an international law firm. India Juris operates through its various offices and affiliates, each of which is a distinct legal entity.
This publication is intended solely for general informational purposes and does not constitute legal, financial, or professional advice. While every effort has been made to ensure the accuracy and reliability of the information contained herein, India Juris makes no representations or warranties, express or implied, as to the completeness or correctness of such information.
The views expressed in this publication are based on the understanding and interpretation of applicable laws and regulations as of the date of publication and are subject to change without prior notice.
Readers are advised to seek independent professional advice before making any decisions or taking any action based on the contents of this publication. India Juris shall not be liable for any loss or damage arising from reliance on the information contained herein or for any actions taken or not taken based on this publication.

© 2026 India Juris. All rights reserved.