
CHILDREN'S DATA PROTECTION UNDER THE DPDP ACT, 2023: A LEGISLATIVE ANALYSIS

Archi Ghiya, LL.M. (Technology & Law), Hidayatullah National Law University,
Nava Raipur, Chhattisgarh, India

Introduction

India's digital infrastructure has expanded rapidly, fundamentally changing how children interact with the online ecosystem. As digital learning, online gaming, social media platforms and e-commerce become deeply embedded in everyday routines, massive quantities of minors' personal information are constantly generated, collected and commercialized. To counter the increasing risks of online exploitation, dynamic behavioral profiling, and algorithmic steering, India passed the "Digital Personal Data Protection Act, 2023 (DPDP Act)"¹. This landmark legislation, primarily focusing on Section 9 of the legislation, provides a specific legal regime for dealing with children's personal data and is operationalized by the Digital Personal Data Protection Rules, 2025².

India's legal framework imposes a mandatory "triple lock" system to protect young users: mandatory verifiable parental consent, harm-centric restrictions on processing data that adversely impacts the well-being of a child, and a strict prohibition on tracking, behavioral surveillance and targeted advertising to minors¹. Although these safeguards reflect a strong legislative commitment to protect children online, they also present complex operational, constitutional and normative challenges. The statute contravenes international human rights standards that recognize the evolving capacities of growing children⁴ by imposing an unflexible age threshold of eighteen years for adulthood, and thus subjecting adolescents to the same restrictions as toddlers.

This report details the legal analysis of privacy of children's data under the DPDP Act, 2023 and the DPDP Rules, 2025. It looks at the governing statutory provisions, procedural rules, relevant constitutional case law, major structural constraints, and key opportunities for policy

¹ Legal Protection of Children's Data under India's Digital Personal Data Protection Act, 2023, 13 Int'l J. Advances Soc. Sci.,no.4,2025.

² Section 9, DPDP ACT

change.

Legislative Context and the Need for Child-Specific Data Protection

Children are a particularly vulnerable population in the digital economy. Unlike adults, young users often lack the cognitive development and critical literacy needed to comprehend data harvesting practices, complex privacy policies, or the long-term implications of creating a permanent digital footprint. Developmental psychology (for example, Jean Piaget's theory of cognitive development) indicates that children in the concrete operational or early formal operational stage cannot think about abstract hazards such as cross-site profiling, algorithmic nudging, and automated behavioral influence. The commercial platforms take full advantage of these cognitive asymmetries through what is known as "dark patterns," rewards, and microtransactions, all designed to enhance user engagement at the expense of privacy and mental wellness. Before the passage of the DPDP Act, there were no specific laws for the protection of data privacy of children in India. Although the "Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" provided general guidelines on online safety and content moderation, they did not provide any regulation on the data processing pipeline that drives digital profiling³.

The Indian Contract Act, 1872 considers any contract made by minors to be null and void ab initio, thereby creating a legal loophole concerning the legal acquisition of data from minors who are devoid of legal capacity to make binding contractual relationships with the platform companies. It is for this reason that Section 9 of the act was drafted to fill these loopholes by formulating one of the strictest laws for child data protection in the world⁴. But comparative analysis reveals a divergence in regulatory philosophy between the Indian framework and leading international regimes:

India (DPDP Act, 2023 & Rules, 2025)- India has one of the most uncompromising regimes in the world. The framework is strictly applicable to all persons below 18 years of age. The framework requires verifiable parental consent before any child's data is processed. It prohibits, under strict penalty, user tracking, behavioral profiling and targeted advertising to minors. The law achieves these protections through an architectural approach that requires

³ How Can 12-13 Year-Olds Have Social Media Accounts?: Supreme Court Orders Centre to Remedy Law for Minors, Hindustan Times (Oct. 17, 2024),

⁴ "Child Data Protection Under DPDP Act: Parental Consent Rules, K&K Legal Services", (last visited sept 25, 2026).

mandatory age-gating and rigid consent verification processes.

European Union (General Data Protection Regulation - GDPR): Within the framework of the EU, the minimum age is under 16 years by default, but Member States may reduce it to 13 years. Processing dependence varies with age, older minors can give direct digital consent, while younger children need parental authorization. The GDPR doesn't impose general bans. Instead, it sets out strict limitations on automated decision-making and profiling that have legal or significant effects. Architecturally, it requires a risk-based approach with Data Protection Impact Assessments (DPIAs) prior to high-risk processing operations¹.

United States (Children's Online Privacy Protection Act – COPPA): Federal US law applies narrowly to children under 13. The regime requires verifiable parental consent as the minimum standard for commercial data collection from young children. Targeted advertising and profiling are only permitted with explicit parental consent, and are strictly prohibited without it. The architectural strategy is mostly sectoral, targeting commercial sites, online services and operators that explicitly target or knowingly collect data from children under 13.

United Kingdom (Age-Appropriate Design Code - AADC): The UK framework applies to all minors under 18 years, and in an effort to ensure the legitimacy of the processing, the UK framework is based on the overarching legal standard of the “best interests of the child” which allows platforms to rely on a variety of processing bases beyond parental consent alone⁵. It imposes serious limitations on high-risk profiling and explicitly prohibits harmful behavioral nudging techniques intended to keep children online. Architecturally, the AADC mandates a “Privacy by Design” philosophy, comprising structural standards that services likely to be used by children need to integrate into their core software design.

While jurisdictions like the EU and US employ flexible or tiered age thresholds that grant older adolescents direct digital agency, India adopts a strict blanket threshold of eighteen years¹.

Moreover, unlike the UK's design-centric model which embeds protection directly into software UX architecture, the DPDP Act relies heavily on formal consent controls⁴.

⁵ Complying with The UK Age-Appropriate Design Code, TrustArc, <https://trustarc.com/resource/uk-age-appropriate-design-code/> (last visited Oct.1, 2026).

Section 9 of the DPDP Act, 2023: Framework

The basic statutory obligations that Data Fiduciaries must comply with while processing the personal data of young individuals are prescribed under Section 9 of the DPDP Act, 2023. The legislative architecture is made up of five interrelated sub-sections that collectively regulate processing preconditions, absolute prohibitions on harm, restrictions on commercial activities and administrative power in relation to exemptions.

Definition of child- Section 2(k) of the DPDP Act specifically defines a “child” as any person who has not attained the age of eighteen years⁶. This provision of the statute enunciates a rigid binary standard:

A person is either an adult with full legal capacity to give independent consent or a minor who must have mandatory parental authorization. The law does not provide for intermediate legal categories, like “mature minors” or adolescents. This bright-line threshold directly correlates with the age of majority under the Indian Majority Act, 1875, the statutory voting age under the Constitution of India, and the protective age boundaries under the Protection of Children from Sexual Offenses (POCSO) Act, 2012⁶.

Verified parental consent- Section 9(1) provides that before processing any personal data of a child or a person with a disability under lawful guardianship, a Data Fiduciary shall obtain verifiable consent from the parent or the legal guardian in the manner prescribed⁶. This statutory requirement is based upon three primary legal elements:

- **Temporal Requirement:** Consent must be secured prior to any data collection or processing activity.
- **Standard of Verification:** Consent cannot be a simple unverified checkbox; the Data Fiduciary must verify that the party granting consent is genuinely the parent or legal guardian.
- **Identity of the Grantor:** Consent is legally sourced from the parent/guardian rather the child, positioning the parent as the sole legal gatekeeper.

⁶ Digital Personal Data Protection Act, 2023 Section 9.

The explanation to Section 9(1) confirms that references to parental consent encompass lawful guardians appointed by courts or statutory bodies, ensuring legal representation for orphans or wards of the state.

Protection of Children's Well-being- Section 9(2) establishes that a Data Fiduciary shall not undertake any processing of personal data that is likely to cause any detrimental effect on the well-being of a child⁶. This represents a harm-based precautionary standard. Unlike Section 9(1), which can be satisfied through procedural compliance, Section 9(2) imposes an absolute, non-negotiable legal prohibition. Processing that inherently causes or is foreseeably likely to cause physical, psychological, social, or economic harm to a child remains illegal even if verifiable parental consent has been granted⁶. The legal burden of proof rests on the Data Fiduciary to demonstrate that its processing operations carry no probable likelihood of detrimental effect.

Section 9(3)–(5) of the DPDP Act, 2023 Tracking, behavioral monitoring and targeted advertising prohibited Section 9(3) imposes a mandatory statutory prohibition on three specific forms of data processing directed at children:

- **Tracking:** The systematic monitoring of an individual's digital actions over time, across multiple websites, mobile applications, or electronic platforms, to assemble browsing histories, spatial movement patterns, or location logs.
- **Behavioral Monitoring:** Collection and analysis of user engagement metrics, online interactions, search histories, or social network data in an effort to develop individual behavioral profiles or psychological characteristics.
- **Targeted Advertising:** Providing targeted commercial content, algorithmic recommendations or promotional advertisements that are based on a child's inferred preferences, habits or historical data footprint.

Government Exemption Powers and Conditional Age Relaxation- Under section 9(4), the Central Government may by notification exempt any class of Data Fiduciaries or processing operations from the obligations imposed under sub-sections (1) and (3). Section 9(5) further creates a statutory incentive structure, whereby the Central Government can notify a lower age threshold for which a Data Fiduciary is not subject to Section 9 duties, if it determines that the

Data Fiduciary processes children's data "verifiably safely".

Rules and Requirements for DPDP Compliance, 2025

The DPDP Rules, 2025 were notified by the Ministry of Electronics and Information Technology (MeitY) on 13th November 2025. The rules set out the technical and administrative requirements for the implementation of section 9. Rules 10 and 12's substantive compliance obligations will be fully effective in May 2027, with an 18-month implementation window.

Procedures for Parent Authentication- Rule 10 operationalizes Section 9(1) by prescribing the technical and organizational mechanisms to be used to obtain "verifiable parental consent"⁷. Under Rule 10, Data Fiduciaries are mandated to take standard due diligence to verify two basic facts: first, that the authorizing individual is an adult (eighteen years of age or above), and second, that such adult is legally identifiable and reachable under applicable law. Platforms will need to put robust identity verification workflows in place to meet Rule 10 requirements before processing data. The verification channels to be used are:

- Authorized parties (through virtual tokens linked to verified identity credentials through official repositories such as DigiLocker) verified.
- Government Identity & Biometric Verification Engagement with government identity verification systems or document verification systems (to the extent permitted by applicable laws relating to mandatory use).
- Financial and Knowledge Based Authentication: This is via micro-transactions initiated by the parent using their credit card authenticated net-banking session or video based KYC process.
- Parent-Child Account Mapping: The direct association between a child sub-account and a parent primary account that is authenticated and active on the same platform or service.

In particular, Rule 10 invalidates unverified self-declaration mechanisms (e.g. unauthenticated

⁷ "WhatsApp's Age Check and the DPDP Act: What Section 9 Means for Children's Data Compliance, AMLEGALS (last visited Oct.2, 2026).

date-of-birth selections or simple age-gate acknowledgment buttons), requiring digital platforms to redesign user onboarding architectures.

Exemptions for Education, Healthcare and Childcare- The requirement of unconditional consent might adversely affect important public services and therefore Rule 12 and Fourth Schedule of DPDP Rules, 2025 provide for some exceptions to Section 9(1) [parental consent requirements] and Section 9(3) [restrictions on tracking]⁸.

DPDP Rules, 2025 - Statutory exemptions

To strike a balance between the need to protect children and the practical operational needs of essential public services, the Fourth Schedule to the DPDP Rules, 2025 creates two targeted exemption categories that exempt certain entities and activities from the strict consent requirements of Section 9(1) and the tracking prohibitions of Section 9(3).

Exemptions Based on Entity (Fourth Schedule, Part A): The institutions specified schools, universities, hospitals, crèches, healthcare centers are exempt from the requirement to obtain verifiable parental consent and to comply with general bans on tracking, for the purposes of their essential functions. This framework facilitates activities such as academic administration, student safety monitoring, medical care and health tracking. This exemption is subject to strict conditions however: processing must be necessary in the interests of education, healthcare or child safety, while commercial profiling, behavioral monitoring and targeted advertising are strictly prohibited.

Purpose-Based Exemptions (Fourth Schedule, Part B): Certain functions are exempt for specific service providers and public welfare bodies, such as those providing school transport, online content filtering, and state aid distribution. Examples of allowed processing activities in this category are real-time GPS location tracking of school transport vehicles, automated filtering of harmful web content, and the delivery of government subsidies or educational certificates. Compliance is subject to a strict purpose limitation: the data processing must be limited to the specific safety/welfare purpose, and location logs or other personal data must be deleted as soon as the specific transport or safety action has been completed⁹.

⁸ Children's Day Under The DPDP Act, 2023 And DPDP Rules, 2025: The New Compliance Frontier for EdTech, Gaming, Social Media and Consumer Platforms, The Legal 500.

⁹ Protecting Children's Data Under the DPDP Rules, IDfy Blog, <https://www.idfy.com/blog/protecting->

Authorized Technical and Safety Processing Functions- Rule 12, except for the institutional exemptions, states that Data Fiduciaries can process the personal data of minors for some specific and narrow technical and safety operations without reference to the prior parental consent.

- Age Assurance and Consent Execution Flow: Digital platforms may collect the minimum amount of personal data needed such as birth dates or parental contact information to determine if a user may be a minor and to execute the Rule 10 consent verification process.
- Child safety and harm prevention: Use of automated content moderation systems and filters to prevent children from accessing explicit, violent or illegal digital content online
- State Welfare Delivery: Processing by instrumentalities of the public sector for the delivery of statutory benefits, educational licenses, subsidies or social welfare entitlements to minors under legal authority

Judicial and Constitutional Framework

Proportionality Test in Puttaswamy The enforceability and validity of Section 9 and the DPDP Rules are subject to scrutiny under the constitutional privacy framework as propounded by the Supreme Court of India. In the case of “*Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)*¹⁰”, a nine-judge Bench unanimously held that the right to privacy is a fundamental right under “Article 21 (Right to Life and Personal Liberty) and Part III of the Constitution”. The Court held that privacy was an integral part of human dignity, personal autonomy and individual liberty. Importantly, the Bench laid down that any State interference with individual privacy has to meet a strict three-fold test of proportionality:

- Legality- The restriction must be based on an express statutory provision.
- Legitimate State Interest- The law must be in furtherance of a legitimate public interest, such as protecting vulnerable minors from digital exploitation.

childrens-data-under-the-dpdp-rules/ (last visited Oct.2, 2026).

¹⁰ (2017) 10 SCC 1.

- Proportionality- The extent of state interference should be reasonably connected to the object sought, the least restrictive means of achieving that object and should be subject to strong legal safeguards against executive abuse.

Section 9 may pass the tests of legality and legitimate aim, but its blanket ban on adolescent digital agency and dependence on mass identity verification creates serious proportionality questions under Article 21.

Puttaswamy (Aadhaar case)- “*In Justice K.S. Puttaswamy (Retd.) v. Union of India (2018)*”¹¹, the issue before the five-judge bench was the validity of the national system of biometric authentication. The Supreme Court of India held that fundamental rights such as the fundamental right to education of a minor under Article 21A can never be made subject to any compulsory disclosure of biometric data or compulsory authentication of identity. The provisions mandating compulsory identity verification for school admissions, competitive exams, and scholarship were struck down on the grounds that non-possession of identity documents or failure to produce the same should never deprive a child of his fundamental rights.

This is directly relevant to the application of the parental consent provision under Rule 10 as well. In the event that online digital services, educational websites and mobile applications mandate compulsory identity-linked authentication as the only valid form of proving parental consent, this could run contrary to the principle of Puttaswamy (II) and be unconstitutional.

In *Nipun Saxena v. Union of India*¹², the Supreme Court considered the privacy rights of vulnerable minors, i.e. victims of sexual violence under child protection statutes. The Court highlighted that the State has an enhanced affirmative obligation under Article 15(3) of the Constitution to protect the anonymity, dignity and identity of a child in all public modes of communication including digital platforms. The decision confirms that children’s privacy interests require a high level of legal protection, giving a strong constitutional support to the strict statutory ban on harmful or detrimental data processing of Section 9(2).

Critical Analysis of the Section 9 & the DPDP Rules, 2025

Despite the strong objective of consumer protection, Section 9 of the DPDP Act and the

¹¹ (2019) 1 SCC 1

¹² AIR ONLINE 2018 SC 826

corresponding 2025 Rules suffer from serious structural and policy shortcomings.

Parental Consent vs. Evolving Autonomy- The main problem with Section 9 is that it has an age limit of eighteen years. The Act does not take into account the international doctrine of ‘evolving capacities’ in Articles 5 and 12 of the UN Convention on the Rights of the Child (UNCRC) and applies the same rules to a seventeen-year-old as to a toddler. Adolescents aged 14 to 17 would require universal parental consent. This creates major societal harms:

- **Digital Gatekeeping:** Teens in vulnerable situations LGBTQ+ youth, victims of abuse, or those seeking reproductive health advice may be cut off from essential support networks if parental consent is required.
- **Socio-Economic Exclusion:** With low levels of online literacy and sharing of devices across households, rural adolescents will be effectively excluded from learning tools and digital opportunities⁴ when complex identity verification requirements are needed.
- **Consent Fatigue.** Parents, bombarded with frequent approval prompts, will predictably give unreflective “click-through” consents, turning a statutory privacy safeguard into an empty legal formality.

Surveillance Risks From Institutional Exemptions- Rule 12 gives operational flexibility for education and transport services. But it also brings in surveillance risks¹³. School software vendors and EdTech platforms collect sensitive data, including learning analytics and real-time location logs. Rule 12 allows invasive monitoring under the guise of “education” or “safety” by completely waiving Section 9(1) consent and Section 9(3) tracking bans for these entities. The statutory language does not clearly define “educational activity,” and platforms are able to monitor student activity without parent knowledge or outside supervision.

The Paradox of Age Verification & Implementation- The implementation roadmap creates significant operational and technical friction. Platforms encounter a “Age Verification Paradox” in determining whether a user is a minor, as they must first collect and verify identity data from all incoming users. This splits traffic into adults and children, triggering the complex workflow of Rule 10 for the latter. This, however, obliges platforms to process government

¹³ DPDP Rules 2025, Explained: Notice, Consent, Security and More, DPDP Act India, <https://dpdpactindia.in/dpdp-rules/> (last visited Oct.2, 2026).

identity documents for their entire user base. The requirement results in mass data over-collection and increases system-wide data breach risks. Non-compliance attracts heavy statutory penalties of up to ₹ 200 crore under Schedule 1 of the DPDP Act.

Suggestive Changes:

India needs to adopt five core structural reforms to address the legal contradictions, practical barriers and constitutional vulnerabilities in the existing child data regime. These are:

Establish a Two-Tier Age Model: Amend Sections 2(k) and 9 to provide for a two-tier system, not a hard eighteen-year cut-off. For 0-12 year olds, we require mandatory parental opt-in and total bans on profiling. 13-17 year olds should be legally capable of giving direct consent to standard digital services, with statutory bans on behavioral tracking, targeted advertising and monetization of data.

Statutory Privacy-by-Design Standards: Introduce mandatory “Child-Centred Privacy-by-Design” standards in the DPDP Rules, based on the UK’s Age Appropriate Design Code (AADC). The law should mandate that digital platforms default to the highest privacy settings, disable exact location tracking, and eliminate dark patterns that try to keep you on the screen longer or get you to share more data than you want to.

Privacy-Preserving Age Assurance: It is imperative that the Ministry of Electronics & IT along with the Data Protection Board of India (DPBI) mandate the use of Zero Knowledge Proofs (ZKPs) and Token-based verification frameworks. The platform can thereby verify the age or legal identity of a person without transmitting, processing or storing the underlying government issued ID credentials, real names or biometrics.

Strict Institutional Exemptions: The regulatory perimeter around the exemption rule 12 is becoming tighter. EdTech companies, educational software platforms, and school transportation services will be required to carry out Mandatory Data Protection Impact Assessment (DPIAs), adherence to strict Purpose Limitation and Automatic Deletion of data when students graduate or complete courses.

Safe proven Section 9(5) Exemptions: The Central Government must invoke Section 9(5) for granting exemptions from behavioural profiling, algorithmic engagement and public content posting at a younger age for digital platforms having technically proven safe

architectures.

Conclusion:

The new section 9 of the Digital Personal Data Protection Act, 2023 along with Rules 10 and 12 of the DPDP Rules, 2025 is indeed a welcome move towards the protection of children from data exploitation and risks online. The blanket prohibitions on behavioral tracking, targeted advertising and data processing set an important benchmark of corporate responsibility of digital companies.

However, the constitutionality and the practicality of this legal framework with its age limit of eighteen years and mandatory consent requirement from the parent has led to significant tensions. This legal framework may end up undermining the very children that it seeks to protect by overlooking their growing autonomy and digitally disenfranchised communities.

As the deadline of May 2027 for implementation of this legal framework approaches, there is a need for policymakers to reconsider the child data governance framework in India. By adopting a tiered approach, ensuring privacy by design compliance and zero knowledge age verification framework, India could effectively strike the right balance between child safety and digital inclusion and constitutional rights.

Bibliography:

1. Indian Statutes

- The Constitution of India, 1950, art. 15(3), 21, 21A.
- The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, §§ 2(k), 9, 9(1)–(5) (India).
- The Indian Contract Act, 1872, No. 9, Acts of Parliament, 1872 (India).
- The Indian Majority Act, 1875, No. 9, Acts of Parliament, 1875 (India).
- The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
- The Protection of Children from Sexual Offences Act, 2012, No. 32, Acts of Parliament, 2012 (India).

2. Rules & Delegated Legislation

- The Digital Personal Data Protection Rules, 2025, rules 10, 12, sch. 4 (India).
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

3. Foreign & International Authorities

- Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (United States).
- Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (European Union).
- Data Protection Act 2018, c. 12, Age Appropriate Design Code (United Kingdom).
- United Nations Convention on the Rights of the Child, arts. 5, 12, *opened for signature* Nov. 20, 1989, 1577 U.N.T.S. 3.