*Page 4117 - 4123*


# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

## [ISSN 2581-5369]

**Volume 9 | Issue 3**

**2026**

# Children's Rights in the Digital Crosshairs: A Comparative Study of Child Data Protection Under India's DPDP Act 2023 and the EU's GDPR Framework

PRIYADARSHINI CHAKRABORTY*

**ABSTRACT**

*The rapid evolution of technology and the pervasive use of data in the digital world have rendered children among the most vulnerable categories of data subjects, or data principals, globally. The Digital Personal Data Protection Act, 2023 represents India's first comprehensive legislative effort to address children's data protection, principally through Section 9. In the European Union, the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA) together constitute the most elaborate children's data governance framework in operation today. This paper undertakes a comparative analysis of these frameworks, examining their structural architecture, age thresholds, consent mechanisms, enforcement postures and underlying normative commitments. It argues that while India's DPDP Act adopts a more protective age threshold than the GDPR, it still suffers from critical implementation gaps, particularly the absence of a specified verification mechanism, the unresolved exemption architecture under Section 9(4), and the absence of any equivalent to the DSA's systemic risk assessment obligations for large platforms. Drawing on the European Commission's July 2025 DSA Guidelines on the protection of minors, the paper proposes a risk-stratified compliance model suited to India's digital ecosystem and recommends specific legislative and regulatory reforms to fortify child data protection in India.*

***Keywords:*** *DPDP Act 2023, Section 9, Children's Data Protection, GDPR, Article 8, Digital Services Act, Verifiable parental consent, Age verification, Data Fiduciary*

## I. INTRODUCTION

In the digital economy, children occupy a paradoxical position. They are among the most enthusiastic consumers of digital services such as social media, gaming platforms, educational applications and e-commerce, yet they possess the least capacity to appreciate the nature, extent and consequences of the processing of their personal data. The commercial logic of platform

* Author is an LL.M. (Data Privacy & IT Law), Manipal Law School, Bengaluru, Karnataka, India.

 [ISSN 2581-5369]

capitalism compounds this vulnerability. Digital platforms derive revenue from attention and behavioural data, and children, with their lower inhibitions and higher engagement rates, are in many situations disproportionately valuable to data-driven business models.

The legislative response to this problem has evolved considerably over the past decade. The United States enacted the Children's Online Privacy Protection Act (COPPA) as early as 1998, restricting data collection from children under thirteen years of age. The European Union addressed children's data through the GDPR in 2018 and, more recently, through the Digital Services Act, 2022, which imposes systemic obligations on 'Very Large Online Platforms' (VLOPs) with respect to minors. The European Commission's Guidelines on the protection of minors under Article 28(1) of the DSA, published in July 2025, represent the most granular regulatory instrument on this subject to date.

India entered this legislative space after a considerable delay. Following six years of consultation and multiple failed Bills, the Digital Personal Data Protection Act, 2023 was finally enacted on 11 August 2023. Section 9 of the Act constitutes its child-specific provision, requiring verifiable parental consent, prohibiting behavioural tracking and banning targeted advertising directed at children. The DPDP Rules, notified in November 2025, added further detail through Rule 10, though significant operational questions remain.

## II. Statutory framework under the DPDP Act, 2023

### A. The statutory obligation

Section 9 of the DPDP Act, 2023 sets out the framework for the protection of children's data. It imposes three key obligations on data fiduciaries.[1]

Under Section 9(1), a Data Fiduciary must obtain verifiable consent from the parent or lawful guardian of the child before processing any personal data of that child.

Section 9(2) prohibits processing of personal data that is likely to cause any detrimental effect on the well-being of a child. This is a broad, principle-based obligation that goes beyond consent, operating as a substantive harm-prevention standard.

Section 9(3) imposes a prohibition on behavioural monitoring, tracking and targeted advertising directed at children.

Section 9(4) carves out exemptions: the Central Government may prescribe certain classes of Data Fiduciaries, or purposes, for which the obligations under Sections 9(1) and 9(3) shall not apply.

[1] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 9(1)–(3) (India).

 [ISSN 2581-5369]

Section 9(5) enables government-notified exemptions for certain Data Fiduciaries that process children's data in a verifiably safe manner, potentially permitting age-appropriate relaxation of the parental consent requirement.

**B. Definition of 'child' and age threshold**

The DPDP Act defines a 'child' under Section 2(f) as any individual who has not completed eighteen years of age. This uniform national threshold is significantly stricter than the GDPR's default of 16 years (with member-state discretion to lower it to 13 years) and broader than the US COPPA standard of 13 years. The Indian legislature's choice of 18 years reflects a protective stance aligned with the age of majority under Indian law and the definition of a minor under the Indian Contract Act, 1872.[2]

This choice has a significant practical consequence. Platforms such as Instagram, Snapchat, YouTube and gaming services, which routinely set their lower age limit at 13 under COPPA, must in India either verify that users are 18 or comply with Section 9's parental consent regime for all users below 18. The compliance burden is substantially higher than under any comparable jurisdiction.[3]

**C. Deficit in the verification mechanism and the unaddressed exemption architecture**

One of the foremost structural gaps in Section 9 lies in its implementation framework. Section 9(1) provides that 'verifiable' parental consent is required but does not prescribe a mechanism for such verification, leaving the answer entirely to subordinate legislation. Rule 10 of the DPDP Rules, 2025 provides for the consent process but does not clarify how a Data Fiduciary is to ascertain that a user is below 18 years of age. Three modalities have been suggested in policy discussions: self-declaration (which is known to be inadequate); Aadhaar-based age-band token verification (which is technically feasible but raises privacy concerns and depends on universal Aadhaar registration); and government-registered Consent Managers. The Ministry of Electronics and Information Technology (MeitY) has yet to issue authoritative guidance on any of these, and this lack of clarity is widely seen as the principal cause of delay in implementing the Act.[4]

---

[2] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 2(f) (India); GAZETTE OF INDIA, Extraordinary, Aug. 11, 2023.

[3] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 2(f) (India). Compare Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 8(1), 2016 O.J. (L 119) 1; Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (COPPA).

[4] The Digital Personal Data Protection Rules, 2025, r. 10, G.S.R. 846(E) (India); *Navigating Children's Privacy and Parental Consent Under the DPDP Act 2023*, THE QUANTUM HUB.

 [ISSN 2581-5369]

Compounding this is the equally uncertain provision for exemptions under Section 9(4). The Central Government has the power to exempt certain categories of Data Fiduciaries and processes from compliance with Section 9. This has the practical effect of leaving organisations in sectors such as education and healthcare, which have legitimate reasons to use children's data, without clear regulation. As the Centre for Communication Governance at National Law University, Delhi has observed, this ambiguity could in fact be detrimental to children's interests, as websites and applications that are genuinely safe for minors may simply block them entirely.[5]

## III. The European framework

### A. GDPR Article 8: consent, age limit and age verification

Article 8 of the GDPR regulates the processing of children's personal data in relation to 'information society services'. Under Article 8(1), such processing is lawful where the child is at least 16 years old; otherwise, consent from the holder of parental responsibility is required. Member States may, however, lower the age limit to no less than 13 years, an option exercised by Ireland, Spain and Sweden, among others. This flexibility acknowledges the difficulties that a fixed age limit of 16 poses for adolescents.

Recital 38 further elaborates that children merit specific protection because they may be less aware of the risks involved in data processing. Critically, Article 8 does not require parental consent for the provision of preventive or counselling services, recognising that requiring it may be harmful in families where abuse occurs, a concern not addressed at all in India's Section 9.[6]

On examination, the GDPR adopts a technology-neutral approach: Article 8(2) provides that reasonable efforts should be made to verify consent, taking into account available technology. What is reasonable depends on the level of risk: the greater the risk, the higher the effort required for verification. Empirical testing illustrates the limits of compliance, showing that all leading platforms used by children, including Instagram, TikTok, Snapchat and YouTube, continue to rely on self-declaration. This offers a critical lesson for India: if self-declaration fails even where enforcement infrastructure exists, India's Rules must be far more prescriptive than the GDPR's standard.[7]

---

[5] Centre for Communication Governance, National Law University Delhi, *Navigating the Indian Data Protection Law: Children's Privacy and the Digital Personal Data Protection Act, 2023* (CCG Blog, Nov. 2023).
[6] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 8(1)–(2), recital 38, 2016 O.J. (L 119) 1.
[7] European Data Protection Supervisor & European Union Agency for Cybersecurity, *EDPS–ENISA Joint Opinion on Age Verification* (2022).

 [ISSN 2581-5369]

### B. The Digital Services Act, 2022 and the July 2025 Guidelines

Beyond the provisions found in the GDPR and the DPDP Act, the DSA introduces an important systemic dimension. Article 28(1) requires providers of online platforms not to present advertising based on profiling to minors. This obligation is operationalised in the Guidelines on Article 28(1) of the DSA (July 2025), in which the European Commission prescribes a range of platform obligations, including:

default private accounts for minors;

no location tracking except where enabled by the user;

disabling compulsive features (such as autoplay, streaks and sleep-hour notifications) by default; and

an annual child safety risk assessment to determine whether protective measures unduly restrict children's rights.[8]

Two aspects of the DSA Guidelines are particularly relevant for comparative law. First, age verification is risk-based, calibrated to the risks that a particular platform poses rather than following a one-size-fits-all solution. Second, the Guidelines introduce the ‘double-blind’ concept, whereby neither the platform nor the age verification service can know the identity of the user being verified.

## IV. Comparative analysis

### A. Minimum age: protection versus autonomy

India's minimum age of 18 years is the most protective in the world; however, the resulting dichotomy leaves much to be desired from an autonomy standpoint. A 17-year-old who wishes to access mental healthcare or civic education, for instance, will require parental consent, and seeking such consent can be dangerous in an abusive or conservative environment. The GDPR's approach, allowing a minimum age to be set at member-state discretion (as low as 13 years), better reflects the evolving capacities of adolescents. The DSA Guidelines go further still, compelling platforms to balance the protection and autonomy of children.

### B. Consent and verification

Both frameworks require parental consent, but they differ in the level of detail demanded. The GDPR's requirement of ‘reasonable efforts’ is technology-neutral and adaptable. The DPDP

[8] European Commission, *Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online under Article 28(1) of the Digital Services Act* (July 14, 2025); Hogan Lovells, *The Long-Awaited EU Guidelines on Article 28(1) DSA: What Online Platforms Must Know* (Aug. 5, 2025).

 [ISSN 2581-5369]

Act's requirement of 'verifiable consent' appears more stringent, yet there is no guidance as to what verifiable consent means. The European experience of over a decade shows that technology neutrality tends to devolve into self-declaration. It is therefore essential that the Indian Rules go beyond this.

### C. Behavioural tracking: absolute versus risk-based

The prohibition on behavioural tracking set out in Section 9(3) makes philosophical sense but is too broad in scope. The DSA bans profiling-based advertising to minors across all platforms, with additional systemic duties for VLOPs. By contrast, India's absolute ban may capture non-advertising contextual recommendations on educational platforms such as YouTube Kids or Byju's.

### D. Platform accountability and systemic responsibilities

The most significant structural flaw in the DPDP Act is the absence of any systemic platform accountability requirement. The DSA mandates that VLOPs undertake annual risk assessments to determine whether the design of their platforms poses any threat to children's safety, engaging with risk at the architectural level of the platform rather than merely at the processing level. The DPDP Rules, 2025 provide for Data Protection Impact Assessment requirements for Significant Data Fiduciaries without tailoring them to the safety risks specific to children. Compulsive design, algorithmic amplification and coercive data extraction are systemic in nature and cannot be resolved through consent and prohibition alone.

## V. Conclusion

The DPDP Rules, 2025 have done more than expected to resolve the problems raised. Rule 10's multi-modal verification framework, and the Fourth Schedule, which provides exemptions for healthcare providers, educational institutions, crèches and transport service providers, address the verification and exemption concerns that scholars had discussed extensively.[9,10]

First, the prohibition on tracking under Section 9(3) needs clarification to distinguish cross-session commercial profiling (the intended target) from same-session contextual personalisation on educational platforms. A targeted notification under Section 9(5), or an amendment to the law, should create an exception in this regard.[11]

Second, although the Data Protection Impact Assessment framework laid down under Rule 13 is comprehensive, it contains no obligation to conduct a child-specific risk assessment.

[9] The Digital Personal Data Protection Rules, 2025, r. 10, G.S.R. 846(E) (India).
[10] The Digital Personal Data Protection Rules, 2025, Fourth Schedule, pts. A & B, G.S.R. 846(E) (India).
[11] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 9(3) (India).

 [ISSN 2581-5369]

Compulsive service design, algorithms that amplify harmful content, and gamified architecture engineered to be addictive can harm a child even without engaging consent or any prohibited activity. Services and applications accessible to children should be required to conduct an annual Child Data Risk Assessment, similar to those under Articles 34 and 35 of the DSA.

India's Section 9, together with the Rules, makes the country one of the most protective children's data frameworks in the world. The implementation window of 18 months from May 2027 is real but limited. If MeitY and the Data Protection Board act on the two focused measures identified above, Section 9 may yet prove true to its promise. If they do not, India will have created a protective framework that ends precisely where the harm begins.

*****

 [ISSN 2581-5369]