World Journal of Law
www.worldlawjournal.com
Online ISSN: 3107-887
Received: 25-06-2026, Accepted: 24-07-2026, Published: 11-08-2026
Volume 2, Issue 3, 2026, Page No. 1-6

Between protection and participation: Rethinking children's privacy and consent in India's digital data protection regime

Dr. Inderjit Kumar[1], Mehak Ahuja[2]
[1] Associate Professor, Department of Law, CT Institute of Law, Jalandhar, Punjab, India
[2] Head HR & Legal, Vienna Advantage (India) Pvt Ltd, Mohali, India

Abstract
Children now learn, play, communicate and create through services that routinely collect personal and behavioural data. These services widen access to education and expression, but they also expose children to profiling, targeted persuasion, dark patterns, image-based abuse and lasting digital footprints. This article asks whether India's child-data framework, centred on verifiable parental consent, adequately protects children while respecting their participation and evolving capacities. It adopts a doctrinal method and examines the Constitution, the UN Convention on the Rights of the Child, General Comment No. 25, the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, the Information Technology Act, 2000 and allied laws. The article finds that parental consent is necessary but cannot carry the full burden of protection. Consent may be hurried, poorly informed or practically compelled, especially when schools require digital platforms. A uniform threshold of eighteen also gives insufficient attention to adolescent maturity, while age verification can itself demand more personal data. The article proposes a four-part child-centric model based on necessity, age-appropriate participation, non-exploitative design and effective remedies. It recommends privacy-protective defaults, child-friendly notices, adolescent assent, limits on profiling, child-rights impact assessments, specific EdTech safeguards and coordinated grievance mechanisms.

Keywords: Children's privacy, digital consent, DPDP act, 2023, parental consent, child autonomy, age-appropriate design

Introduction

For many children, an ordinary day now begins and ends with a digital service. A school application records attendance and homework. A video platform learns viewing preferences. A game tracks play, purchases and social interaction. A messaging service stores photographs, contacts and location signals. Each use may appear routine, yet together these activities create a detailed account of the child's habits, relationships, abilities and vulnerabilities. Digital participation has therefore made childhood increasingly data-intensive [1].

The benefits are substantial. Online services can support education, creativity, communication and access to information. The same services, however, may expose children to cyberbullying, grooming, non-consensual image sharing, harmful recommendations, behavioural monitoring and commercial persuasion. Official data captures only part of this problem. NCRB figures placed before Parliament show that registered cyber-crime cases against children increased from 232 in 2018 to 1,823 in 2022 [2]. Many privacy harms never appear in crime statistics because they result from lawful but opaque practices such as profiling, prolonged retention and design that encourages disclosure.

These risks require more than parental supervision. Decisions about a child's data are also made by schools, EdTech providers, gaming companies, advertisers, social media platforms and algorithmic systems. Their choices determine what is collected, which settings are offered, how long data is retained and whether a child is nudged towards public sharing or continued engagement. The problem is therefore institutional as well as personal.

Indian law now addresses parts of this landscape. The Digital Personal Data Protection Act, 2023 (DPDP Act) creates specific duties for processing children's personal data. The Information Technology Act, 2000 and the intermediary rules deal with content-related harms, platform due diligence and grievance redressal. POCSO, education law and consumer protection rules provide further safeguards. These laws perform different functions, but they do not yet operate as a single child-rights framework.

Research Question, Method and Argument

This article asks a focused question: can a framework built primarily around verifiable parental consent protect children's privacy without overlooking their voice and developing autonomy? It answers that question only partly in the affirmative. Parental involvement is important, particularly for younger children, but consent alone cannot correct unequal bargaining power, inaccessible notices, manipulative design or compulsory use of digital services.

The article uses a doctrinal and analytical method. It reads the DPDP framework alongside constitutional privacy, the UN Convention on the Rights of the Child (UNCRC), General Comment No. 25 and allied Indian legislation. Its purpose is to identify the central legal gaps and offer a workable model for reform.

The argument proceeds in four steps. First, children must be treated both as persons requiring special protection and as rights-holders entitled to participation. Secondly, India's new data-protection regime is a significant advance, but its key child-data duties remain in transition and its consent model has structural limits. Thirdly, those limits are most visible in age assurance, EdTech, dark patterns and

fragmented remedies. Finally, India should move from consent-centred compliance to child-centred accountability based on necessity, age-appropriate participation, non-exploitation and effective redress.

Children's Digital Rights: Protection, Privacy and Participation

1. The Child as a Rights-Holder

The UNCRC changed the legal understanding of childhood. It did not reject protection; instead, it placed protection within a broader account of dignity, development and participation. The Convention requires the child's best interests to be a primary consideration, recognises parental guidance in accordance with evolving capacities, protects privacy and gives the child a right to be heard in matters affecting her [3]. These principles apply online as fully as they apply offline.

General Comment No. 25 makes that point explicit. It states that children's rights must be respected, protected and fulfilled in relation to the digital environment. It also treats privacy as important to children's agency, dignity and safety, and asks States to consider the effects of platform design, profiling and commercial practices [4]. The child is therefore not merely a potential victim of online harm. She is also a learner, speaker, creator and participant whose access to digital spaces has independent value.

This dual status explains the title of this article. Protection without participation can become excessive control. It may justify blanket restrictions, constant parental surveillance or the exclusion of adolescents from decisions about their own identity. Participation without protection can be equally harmful if platforms treat children as ordinary consumers capable of bearing every informational risk. Child-rights law requires a position between these extremes.

2. Privacy, Dignity and Evolving Capacities

For a child, privacy is not simply secrecy. It creates room to form friendships, test ideas, make mistakes and develop an identity without every act being permanently recorded or commercially evaluated. Data collected during childhood may remain available long after majority. School performance, health information, photographs, search histories and gaming behaviour can shape how the person is understood in the future.

The constitutional basis for this protection lies principally in article 21. In *Justice K.S. Puttaswamy (Retd.) v. Union of India* [5], the Supreme Court recognised privacy as intrinsic to life and personal liberty and treated informational privacy as part of dignity and autonomy. The judgment also acknowledged that modern privacy threats arise from private entities as well as the State. That observation is particularly important when children's daily lives are mediated by commercial platforms.

Other constitutional provisions reinforce this reading. Articles 14 and 15(3) support equal and child-specific protection. Article 19(1)(a) protects expression and access to information. Article 21A links digital education with the right to education, while articles 39(e) and 39(f) direct the State to protect childhood from abuse and exploitation and to secure development in conditions of freedom and dignity [6]. The constitutional objective is not simply to keep children offline; it is to make participation safer and fairer.

The principle of evolving capacities supplies the bridge between protection and autonomy. A young child may need close parental mediation. An older adolescent may understand a low-risk service and should be informed and heard. Age does not remove vulnerability, but maturity should affect how information is presented and how decisions are made. The legal task is to vary participation without weakening the platform's independent duty of care.

The best-interests principle should not become an unreasoned slogan. A regulator should identify the concrete interest at stake, consider less intrusive alternatives and explain how safety is balanced with privacy, expression and access. This discipline matters because measures presented as protective - continuous location tracking, biometric attendance or intrusive parental-control tools - can themselves interfere with a child's rights.

India's Legal and Regulatory Architecture

1. The DPDP Act and the 2025 Rules

The DPDP Act is India's most direct law on children's personal data. It applies to digital personal data processed in India and, in defined circumstances, to processing outside India connected with offering goods or services to persons in India. It defines a child as an individual below eighteen and uses broad definitions of personal data and processing [7]. The regime can therefore cover obvious identifiers as well as device data, learning analytics, location histories and inferred preferences.

Section 9 is the central child-specific provision. It requires a Data Fiduciary to obtain verifiable parental consent before processing a child's personal data. It separately prohibits processing likely to cause a detrimental effect on the child's well-being and prohibits tracking, behavioural monitoring and targeted advertising directed at children, subject to statutory exceptions [8]. This structure is important: parental consent cannot validate every practice. Some duties exist independently of consent.

The provision nevertheless leaves difficult questions. The Act does not define "detrimental effect on well-being". Nor does it provide an age-sensitive test for distinguishing an educational recommendation from behavioural monitoring, or ordinary personalisation from targeted persuasion. Section 9 also permits exemptions for prescribed classes and purposes, and allows the Government to relax specified duties for processing that is "verifiably safe". These powers require transparent criteria and narrow use [9].

The Act gives Data Principals rights to information, correction, updating, erasure and grievance redressal. A breach of the additional duties relating to children may attract a penalty of up to two hundred crore rupees [10]. Yet, for a child, these rights will usually be exercised through a parent or lawful guardian. The effectiveness of the scheme thus depends on adult awareness and on procedures that are simple enough to use.

The Digital Personal Data Protection Rules, 2025 add operational detail. Rule 3 requires a clear and understandable notice that identifies the data and purposes of processing. Rule 10 requires technical and organisational measures for verifiable parental consent and due diligence to confirm that the person claiming to be the parent is an identifiable adult [11]. The rule permits reliance on available identity and age details or on voluntarily provided details, including a virtual token from an authorised entity.

Two gaps remain. First, a notice may be clear to an adult and still be inaccessible to a child. Rule 3 does not expressly require age-layered, visual or child-friendly explanations. Secondly, rule 10 concentrates on adult identity and age; the reliability of the claimed parental relationship is left largely to the fiduciary's chosen measures. Verification may therefore vary considerably across services.

Rule 12 creates conditional exemptions for specified health, education, childcare, transport and safety contexts. Rule 13 requires Significant Data Fiduciaries to conduct annual data-protection impact assessments and audits, and to examine whether algorithmic software is likely to pose a risk to Data Principals' rights [12]. These provisions can support legitimate services, but educational or safety exceptions should not become routes for commercial profiling or indefinite retention.

The timing of the regime also matters. The Act and Rules were brought into force through a staggered schedule. As of June 2026, section 9 and the principal operational rules on notice, consent and children's data remained within the eighteen-month transition period [13]. The present article therefore evaluates an enacted and notified framework whose central child-data duties are not yet fully operational. This transition offers a valuable opportunity to issue child-specific guidance before compliance becomes mandatory.

That guidance should clarify the meaning of harm to well-being, the boundary between personalisation and behavioural monitoring, acceptable forms of age assurance and the evidence required before a service is treated as verifiably safe. Clear examples would reduce uncertainty for legitimate providers while making it harder to disguise commercial profiling as a safety or educational function.

2. The IT Act and Allied Protections

The DPDP Act regulates personal data, but many online harms are content-related. The Information Technology Act, 2000 therefore remains relevant. Section 66E addresses certain privacy violations involving images of private areas; section 67B addresses electronic material depicting children in sexually explicit acts; section 69A authorises blocking in specified circumstances; and section 79 provides conditional safe harbour to intermediaries [14]. These provisions do not form a child-data code, but they address abuse that consent law alone cannot reach.

The Intermediary Guidelines and Digital Media Ethics Code Rules, 2021 add due-diligence and grievance duties. They require intermediaries to publish user rules, act on complaints and take specified measures against unlawful or harmful content. Following the 2026 amendments, complaints concerning intimate imagery, nudity, sexual content or electronic impersonation must be acted on within two hours. The amendments also impose duties relating to unlawful synthetically generated information and labelling of other synthetic audio-visual content [15]. These rules are directly relevant to morphed images, deepfakes and AI-generated sexual abuse material involving children.

POCSO supplements this framework by criminalising the use of a child for pornographic purposes and by providing child-sensitive reporting and trial procedures [16]. Consumer protection law addresses a different problem: manipulation before the user agrees. The CCPA Guidelines on Dark Patterns identify practices such as false urgency, forced action, confirm shaming and interface interference [17]. Such techniques can influence a child to disclose data or influence a parent to choose a privacy-invasive setting.

Education law adds another dimension. When a school requires an application for attendance, homework or assessment, a parent may have no realistic option to refuse. The right to education cannot depend on accepting unnecessary tracking or unrelated commercial use of student data [18]. The legal issue in such cases is not only whether consent exists, but whether the collection is necessary for the educational purpose.

3. A Fragmented System

India therefore has several relevant laws, but they are organised around different harms and institutions. A data leak may involve the DPDP framework. A morphed image may require an intermediary complaint and police action. Sexual exploitation may invoke POCSO. A school platform may involve education authorities and a vendor contract. A deceptive interface may raise a consumer complaint.

Specialised laws are not inherently problematic. The difficulty arises when a child or parent must identify the correct authority while harm is spreading. Fragmentation can also allow each actor to define its responsibility narrowly. A platform may point to parental consent, a school to educational necessity and a vendor to its contract. A coherent framework must connect these duties through the best interests of the child and provide a clear route to redress.

A sensible division of labour is possible. Data-protection authorities can address collection, retention and profiling; intermediaries can provide rapid content remedies; police and POCSO institutions can investigate offences; and education authorities can regulate school procurement. What is missing is a referral protocol and shared child-safety standards that prevent gaps between these institutions.

Why Parental Consent is not Enough

1. The Illusion of Informed Choice

Consent assumes that the person deciding has understandable information and a genuine choice. Online, both assumptions are often weak. Privacy notices are lengthy, future uses of data are uncertain, and services are offered on standard terms. The user can click "accept" but cannot negotiate. This is the familiar problem of privacy self-management: too many complex choices are transferred to individuals who have less information and less power than the entity seeking consent [19].

Parental consent does not remove that structural imbalance. A parent may authorise an educational app because a teacher requires it, or a messaging platform because it is the child's main means of social contact. The decision may be reasonable, yet it is not necessarily informed or freely negotiated. Consent can then become proof of compliance rather than a reliable measure of the child's best interests.

Digital literacy further complicates the issue. The ability to install an application does not imply an understanding of ad-tech, cloud storage, recommender systems or inferred data. Children may be technically confident but unaware of how their attention is monetised. Parents may understand the immediate function of a service but not its data ecosystem. Protection cannot therefore depend on every family successfully decoding platform architecture.

2. A Single Age and the Age-Assurance Paradox

The DPDP Act's age of eighteen offers clarity and strong coverage. It also treats a six-year-old and a seventeen-year-old in the same way for consent. That approach may be suitable for high-risk commercial practices, but it is less convincing for every low-risk decision concerning learning, creativity or expression. The UNCRC's principle of evolving capacities requires the child's developing understanding to receive increasing weight [20].

This does not justify lowering protection for adolescents. It supports a distinction between legal consent and meaningful assent. While the statute requires parental consent, a service used by older children should also explain the processing directly to them and obtain an affirmative, age-appropriate indication of agreement. The platform's duties should remain unchanged even when both parent and child agree.

Verification creates a second problem. To determine that a user is a child and that the consenting person is an adult, a platform may request identity details, a government document, a facial estimate or a third-party token. The measure intended to protect privacy can therefore generate more data and another security risk. This is the age-assurance paradox.

The answer is not to abandon age assurance, but to make it proportionate. A service should use the least intrusive method reasonably available, store no more proof than necessary and prohibit reuse of verification data for advertising or analytics. The proportionality reasoning in *Puttaswamy* supports that approach: a legitimate protective aim does not excuse an unnecessarily intrusive method [21].

3. EdTech, Dark Patterns and Design-Based Harm

The limits of consent are especially visible in EdTech. A school can create practical compulsion by requiring one platform for classes, assessment or communication. The child cannot meaningfully bargain, and the parent may fear that refusal will affect education. In this setting, the lawful basis and safeguards should turn on necessity and the school's duty towards the child, not on a broad consent form.

Student data also deserves careful treatment because it can reveal far more than marks. Patterns of response, time spent on a task, accessibility needs and teacher observations may support learning, but they may also be used to rank, predict or label a child. Schools should not permit vendors to use such data for advertising, unrelated product development or profiles that follow the child beyond the educational relationship.

Dark patterns show how interface design can undermine choice. A bright "continue" button, a hidden refusal option or a warning that privacy settings will reduce enjoyment can steer both children and parents. The legal question should be whether the design preserved freedom of choice, not merely whether a box was ticked. Consent produced by manipulation should carry little regulatory weight.

The same point applies to recommender systems. A platform may describe its activity as personalisation rather than behavioural monitoring, while still using observed behaviour to maximise engagement or shape purchases. Regulators should look at function rather than label. Where a system predicts and exploits a child's vulnerability, consent should not make the practice acceptable.

4. Remedies That Children Can Actually Use

A right to erasure or a grievance process is of limited value if a child cannot find it. Online harm can spread quickly, particularly where an image, location or impersonation is involved. A family may need removal, preservation of evidence, police assistance and data correction at the same time. Separate portals and technical forms increase delay.

Remedies must therefore be visible, simple and coordinated. Children should be able to report harm in plain language and in regional languages. Platforms should distinguish urgent safety complaints from ordinary service disputes. Authorities should refer complaints to the correct institution rather than requiring the child to begin again. The system should be organised around the harm suffered, not around administrative boundaries.

A Four-Part Child-Centric Model for India

Comparative law offers useful techniques, although no foreign model should be copied mechanically. The United Kingdom's Age-Appropriate Design Code places the child's best interests at the centre of service design. Article 8 of the EU GDPR uses a graded approach to children's consent, while the United States' COPPA framework imposes special duties on services directed to younger children [22]. The common lesson is that consent must be supported by design duties, risk controls and enforcement.

India can express that lesson through a four-part test. Any digital service likely to be accessed by children should be assessed for necessity, age-appropriate participation, non-exploitation and effective remedy. These elements are not substitutes for the DPDP Act. They provide a practical method for interpreting and implementing it.

1. Necessity: Collect Less and Protect by Default

The first question should be simple: is the data genuinely necessary for the service offered to the child? An educational app does not ordinarily need the child's contact list or precise location. A game should not collect unrelated browsing history merely because it may have future commercial value. Data minimisation should be applied at the design stage, before consent is requested.

Privacy-protective settings should also be the default. Public profiles, precise geolocation, stranger messaging, contact discovery and personalised advertising should be disabled unless a clear child-rights justification exists. Retention should be limited, and inactive accounts should not become permanent archives of childhood. A child should not have to trade privacy for ordinary participation.

India should issue an age-appropriate design code under the combined authority of data-protection, intermediary and consumer law. The code should specify minimum defaults while allowing proportionate technical solutions. It should apply to services directed to children and to general services that are reasonably likely to be accessed by them.

2. Age-Appropriate Participation: Notice, Consent and Assent

The second question is whether the child can understand and participate in the decision. Notices should be layered. A short first layer should state what data is collected, why it is needed, who receives it and how it can be deleted. Visual prompts, audio explanations and regional languages should

be used where appropriate. The full legal notice can remain available without becoming the only source of information.

For younger children, parental consent and strong defaults should remain central. For older adolescents, the current statutory requirement of parental consent should be supplemented by the child's assent for ordinary services. High-risk processing - including precise location, biometric data, public posting, commercial profiling or third-party sharing - should attract strict safeguards that cannot be waived by either parent or child.

Essential services require a separate approach. Schools and healthcare providers should offer a privacy-preserving route to access rather than a choice between broad data use and exclusion. Refusal of optional analytics or commercial uses should not result in denial of education, care or child-protection support.

3. Non-Exploitation: Design Duties and Accountable Algorithms

The third question is whether the service profits from or amplifies a child's vulnerability. Section 9's restrictions on tracking, behavioural monitoring and targeted advertising provide a strong starting point [23]. Implementation guidance should make clear that a change of label does not change the substance. "Personalisation" and "engagement optimisation" should be examined where they rely on behavioural profiles or persuasive targeting.

Dark patterns should be treated as relevant to the validity of consent and not only as a consumer-law issue. Child-facing services should test whether interface choices pressure users, hide protective options or encourage excessive disclosure. Regulators should be able to require design changes, not merely a revised privacy policy.

Rule 13's impact-assessment and algorithmic due-diligence duties should be developed into a child-rights impact assessment for high-risk services [24]. The assessment should examine data collection, profiling, harmful recommendations, addictive features, stranger contact, discrimination and complaint pathways. A public summary and independent audit should be required where the risk is substantial.

4. Effective Remedy: Sector Rules, Coordination and Literacy

The fourth question is whether a child can obtain timely help. India needs a one-door referral model. A complaint made to a platform, the Data Protection Board, a cyber-police portal or a child-rights authority should be capable of referral to the correct body without repeated filing. Urgent cases involving intimate imagery, grooming, impersonation or location exposure should receive priority and trained review.

EdTech requires specific standards. Schools should publish a student-data policy, carry out due diligence before selecting vendors and include contractual limits on purpose, sharing, security and retention. Vendors should be barred from advertising to students or using school data for unrelated commercial profiles. When the relationship ends, the default should be secure deletion rather than indefinite storage.

Remedy also includes the ability to correct and outgrow a digital past. Children and parents need a practical process to remove obsolete profiles, inaccurate inferences and content posted during childhood. Platforms should explain these rights in language a child can understand and provide status updates during the complaint process.

Finally, law must be supported by digital literacy. Children, parents and teachers should learn not only about screen time and cybercrime, but also about permissions, data trails, dark patterns, synthetic media and reporting tools [25]. Literacy cannot replace regulation, but it helps rights-holders recognise when protection has failed.

Together, the four elements change the regulatory question. Instead of asking only whether a parent authorised processing, the decision-maker asks: Was the data necessary? Was the child informed and heard in an age-appropriate way? Did the design avoid exploitation? Could the child obtain an effective remedy? A service that fails these questions should not be treated as child-safe merely because it possesses a consent record.

Conclusion

India's emerging child-data framework is an important advance. The DPDP Act recognises children as a distinct class of Data Principals and places limits on harmful processing, tracking and targeted advertising. The IT Act, intermediary rules, POCSO and consumer law address content abuse, platform responsibility and manipulative design. These measures create a foundation, but not yet a coherent system.

The central weakness is the expectation that parental consent can carry too much regulatory weight. Consent may be poorly informed, shaped by interface design or practically compelled by education and social participation. A uniform age threshold also risks overlooking adolescent maturity, while intrusive age assurance can create fresh privacy risks. These are structural problems, not failures of individual parenting.

The answer is not to abandon parental involvement. It is to place consent within a wider framework of institutional responsibility. Necessity, age-appropriate participation, non-exploitation and effective remedies provide a clear basis for that framework. They protect younger children through strong defaults, recognise the voice of adolescents and keep responsibility on the entities that design and profit from digital services.

A child-centred regime should enable children to learn, create and communicate online without making surveillance or manipulation the price of access. Indian law should therefore move beyond the narrow question of who clicked "I agree". The better question is whether the service was designed, operated and supervised in a manner consistent with the child's dignity, safety, privacy and evolving autonomy.

References

1. Committee on the Rights of the Child, General Comment No. 25 on Children's Rights in Relation to the Digital Environment, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).
2. Ministry of Home Affairs, Government of India, "Cyber-crime Targeting Children," Press Information Bureau (July 29, 2025), Release ID: 2149788.
3. Convention on the Rights of the Child, 1989, arts. 3, 5, 12 and 16.

4. Committee on the Rights of the Child, General Comment No. 25 on Children's Rights in Relation to the Digital Environment, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).
5. (2017) 10 SCC 1.
6. The Constitution of India, arts. 14, 15(3), 19(1)(a), 21, 21A, 39(e) and 39(f).
7. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 2(f), 2(t), 2(x) and 3.
8. Id., s. 9(1)-(3).
9. Id., s. 9(4)-(5).
10. Id., ss. 11-13 and Schedule, serial no. 3.
11. The Digital Personal Data Protection Rules, 2025, rr. 3 and 10.
12. Id., rr. 12-13 and Fourth Schedule.
13. Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), Gazette of India, Extraordinary, Part II, sec. 3(i) (Nov. 13, 2025).
14. The Information Technology Act, 2000 (Act 21 of 2000), ss. 66E, 67B, 69A and 79.
15. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(2)(b), 3(3) and 4(1A), as amended by G.S.R. 120(E) (Feb. 10, 2026).
16. The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012), ss. 13-15, 19 and 33-38.
17. The Consumer Protection Act, 2019 (Act 35 of 2019), s. 18; Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023, Annexure I.
18. The Constitution of India, art. 21A; The Right of Children to Free and Compulsory Education Act, 2009 (Act 35 of 2009).
19. Daniel J. Solove, 'Privacy Self-Management and the Consent Dilemma' 126 Harv. L. Rev. 1880 (2013).
20. Convention on the Rights of the Child, 1989, art. 5; Committee on the Rights of the Child, General Comment No. 25 on Children's Rights in Relation to the Digital Environment, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).
21. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.
22. Information Commissioner's Office, Age Appropriate Design: A Code of Practice for Online Services (2020); Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 8; Children's Online Privacy Protection Act, 15 U.S.C. ss. 6501-6506.
23. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 9(3).
24. The Digital Personal Data Protection Rules, 2025, r. 13.
25. Committee on the Rights of the Child, General Comment No. 25 on Children's Rights in Relation to the Digital Environment, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).