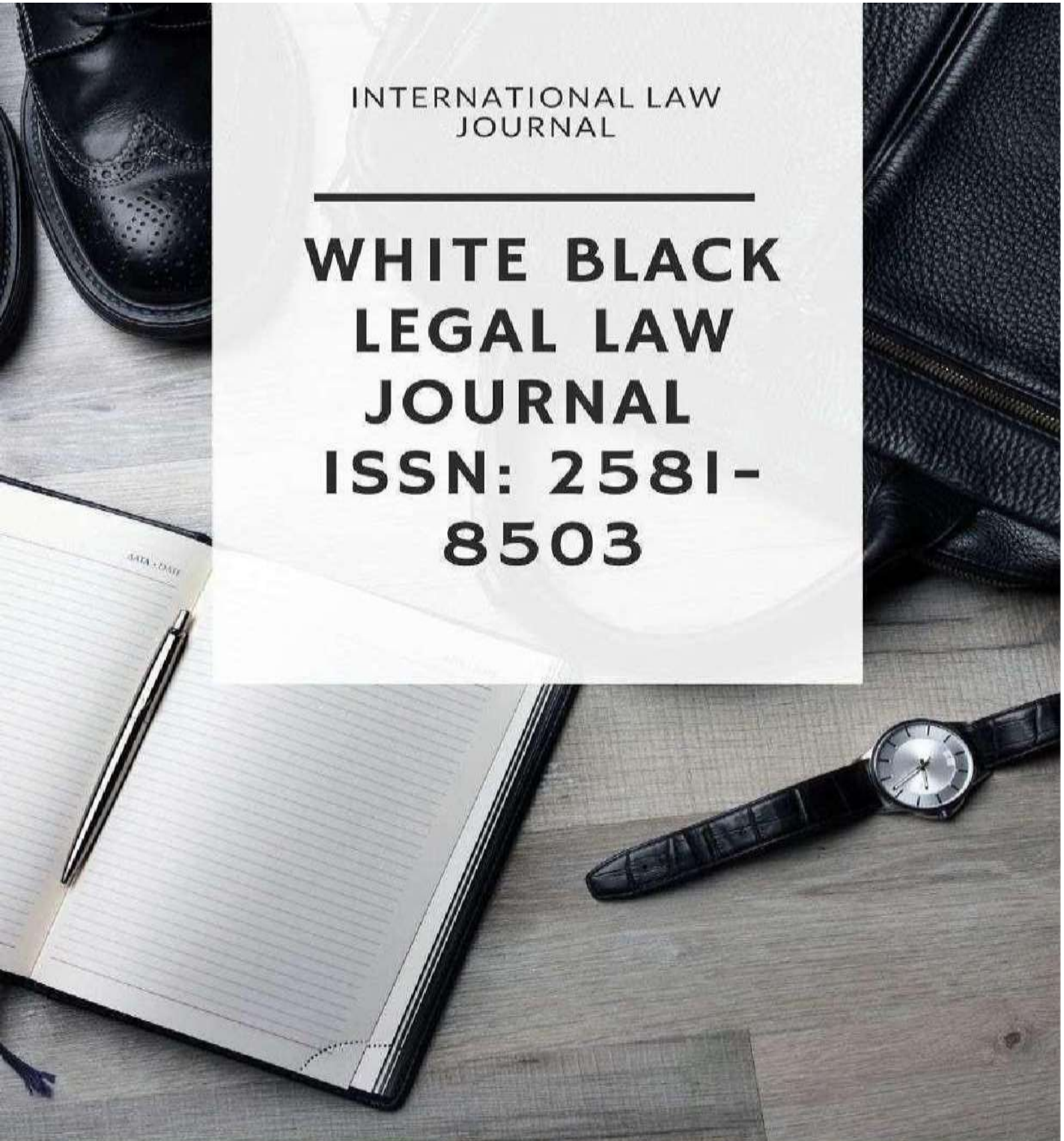




INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

THE AGE OF CONSENT PARADOX EVALUATING INDIA'S DPDP ACT ON MINOR BEHAVIOURAL MONITORING AND VERIFIABLE CONSENT AGAINST GDPR STANDARDS

AUTHORED BY - SAMBAVI PARAMESWARAN

[B.com LLB hons SASTRA UNIVERSITY] · Cyber Law Research Paper

ABSTRACT

This paper offers a socio-legal critique of how India's Digital Personal Data Protection Act, 2023 (DPDP Act) treats the personal data of children, concentrating on Section 9. That provision requires a Data Fiduciary to obtain verifiable parental consent (VPC) before handling a child's data and, subject to limited exemptions, forbids tracking, behavioural monitoring and targeted advertising aimed at children, who under Section 2(f) are all persons below eighteen. Read with the consent standard in Section 6, the notice duties in Section 5, the general obligations in Section 8 and the penalty machinery in Section 33, the scheme is meant to shield minors from commercial exploitation. The paper contends, however, that neither the Act nor the notified DPDP Rules, 2025 (Rule 10 in particular) defines several of the terms on which the scheme turns, namely "verifiable" consent, "tracking or behavioural monitoring", "targeted advertising" and "lawful guardian", and that neither offers a risk-proportionate test for recognising a child or confirming a parent's consent. This uncertainty pulls Data Fiduciaries in opposite directions. Some will over collect identity documents, age proofs and behavioural signals to prove diligence, which conflicts with data minimisation. Others will under comply through ceremonial measures such as self declared ages, leaving children largely unprotected. Using comparative doctrinal analysis supported by illustrative compliance scenarios, the paper sets India's flat eighteen year threshold against the age-tiered approach of Article 8 GDPR and the principles in Articles 5 and 25, and asks whether risk proportionate verification and age-appropriate design can offer a remedy.

Keywords: *Verifiable Parental Consent (VPC); DPDP Act 2023; Section 9 DPDP Act; DPDP Rules 2025; Rule 10; behavioural monitoring of minors; definitional gaps; over-collection; under-compliance; data minimisation; verification paradox; age verification; GDPR Article 8; comparative legal analysis; Data Fiduciary obligations; minor data protection in India.*

I. INTRODUCTION

Much of childhood in India now unfolds on data-driven platforms: social networks, online games and learning apps. The Digital Personal Data Protection Act, 2023 (DPDP Act) addresses this reality in Section 9. The provision necessitates a Data Fiduciary to obtain verifiable consent from a parent or lawful guardian of the child before processing the child's personal data, and it prohibits, subject to limited exemptions, tracking, behavioural monitoring and targeted advertising directed at children.¹ The Act treats every person under eighteen as a child,² a cap well above the thirteen-to-sixteen range permitted by the European Union's General Data Protection Regulation (GDPR).³ Read at face value, the regime is very protective and unusually stringent.

The difficulty lies in how these duties are drafted. The Act does not define what makes a consent "verifiable", what amounts to "tracking or behavioural monitoring" or "targeted advertising", or how a fiduciary has to decide that a particular user is a child. The Digital Personal Data Protection Rules, 2025 (DPDP Rules), notified in November 2025, add some operational detail. Rule 10 lays ways of confirming that the person giving consent is actually an identifiable adult, among them reliable identity and age details and virtual tokens issued by authorised entities such as Digital Locker service providers.⁴ Yet these Rules lay down methods rather than a standard, and the central terms remain unaddressed.

This paper discusses that these gaps push Data Fiduciaries in two opposite directions. Where the standard is unclear and the penalty is heavy, a cautious fiduciary may over-collect: it may verify every user, demand identity documents from parents and children, and even profile behaviour in order to work out who is a child. That course sits uneasily with the necessity limit in Section 6(1) and with the principle of data minimisation. A less cautious fiduciary may under-comply, relying on a tick-box, a self-declared age or a narrow reading of "monitoring", which leaves the child effectively unprotected. Both outcomes defeat the core purpose of Section 9. The paper calls this the dual-failure thesis.

Three research questions structure the inquiry:

1. Which key terms in Section 9 and Rule 10 are undefined or under-specified?
2. How do these gaps encourage over-collection of personal data for parental consent and age assurance?
3. How do they encourage under-compliance with the consent and anti-monitoring duties, and can the GDPR's risk-proportionate approach offer a way out?

The study adopts a comparative doctrinal method. It analyses the text of the Act and the Rules

and compares India's regime with the GDPR (Articles 5, 8 and 25) and, where useful, with the UK Age-Appropriate Design Code, the EU Digital Services Act and the US Children's Online Privacy Protection Act (COPPA). One limitation should be stated plainly at the outset. The core Rule 10 obligations are expected to become enforceable only after the eighteen-month phase-in, around May 2027, so there is no observed compliance behaviour on which the paper can rely.⁵ The argument is therefore structural. It analyses the incentives that the present drafting creates and tests them against illustrative scenarios from education, gaming and social media, each of which is presented openly as a hypothetical.

The paper proceeds in nine parts. Part II discusses the statutory framework and Part III reviews the literature. Part IV maps the definitional gaps. Parts V and VI examine over-collection and under-compliance in turn. Part VII draws on the comparative model, Part VIII gives recommendations, and Part IX concludes.

II. STATUTORY AND REGULATORY FRAMEWORK

A. The Act: the general consent architecture

The DPDP Act mainly involves two parties: the Data Principal, the party to whom the data relates, and the Data Fiduciary, the party or the entity that decides why and how that data is processed. Four provisions form the background against which Section 9 operates.

First, Section 2(f) defines a "child" as an individual who has not completed eighteen years of age.⁶ The definition is flat. It contains no age brackets and makes no distinction between a seven year old and a seventeen year old.

Second, Section 5 requires a fiduciary to give notice when it asks for consent, identifying the personal data sought, the purpose of processing and the manner in which the individual may exercise her rights.⁷

Third, Section 6 sets general standard for consent: it must be free, specific, informed, unconditional and unambiguous, and it must be signified by a clear affirmative action. Section 6(1) further confines consent to the personal data necessary for the specified purpose.⁸ This necessity limit is the Act's own version of data minimisation, and it becomes central to the over collection argument in Part V.

Fourth, Section 8 imposes general duties on fiduciaries, including reasonable security safeguards, notification of personal data breaches and erasure of data once its purpose has been served.⁹

B. Section 9: the children's provision

Section 9 adds a heightened layer of protection for children and for persons with disabilities who act through a lawful guardian. In summary:¹⁰

- Section 9(1) requires the fiduciary, before processing a child's personal data, to obtain verifiable consent from the parent or lawful guardian.
- Section 9(2) bars any processing that is likely to have a detrimental effect on the child's well-being.
- Section 9(3) bars tracking, behavioural monitoring and targeted advertising directed at children.
- Section 9(4) allows the Rules to exempt prescribed classes of fiduciaries, or prescribed purposes, from sub-sections (1) and (3).
- Section 9(5) empowers the Central Government to notify, for a fiduciary whose processing of children's data is shown to be "verifiably safe", an age below eighteen above which that fiduciary is released from the obligations in sub-sections (1) and (3).

The prohibition in Section 9(3) is therefore strong but not absolute. It coexists with a power to create exemptions, and this matters for what follows, because it is the exemption structure, and not the prohibition alone, that determines how much guesswork a fiduciary must do.

C. Enforcement: Section 33 and the Schedule

The Data Protection Board of India enforces the Act. Under Section 33, once it has held an inquiry the Board may impose a monetary penalty of the kind specified in the Schedule to the Act.¹¹ The Schedule places the maximum penalty for breach of the additional children's-data obligations under Section 9 at ₹200 crore, which is among the highest tiers in the statute.¹² The relevant point for this paper is that a severe penalty is attached to duties whose key terms are left undefined.

D. The DPDP Rules, 2025

The Rules were notified in November 2025, following consultation on a published draft.¹³ Three provisions matter here.

Rule 10 (verifiable parental consent). The Rule requires the fiduciary to adopt appropriate technical and organisational measures so that verifiable parental consent is obtained before a child's data is processed. It also requires due diligence to confirm that the person claiming to be the parent is an identifiable adult.¹⁴ Several routes are contemplated: reliance on reliable

identity and age details already held by the fiduciary, details voluntarily furnished by the parent, or a virtual token, mapped to identity and age, issued by an authorised entity, including through a Digital Locker service provider.¹⁵

Rule 11 (persons with disabilities). This extends comparable consent requirements to cases in which a lawful guardian acts for a person with a disability.

Rule 12 and the Fourth Schedule (exemptions). These give effect to Section 9(4). Part A exempts certain classes of fiduciary, such as healthcare providers, educational institutions, crèches and child transport services. Part B exempts certain purposes, including the discharge of legal duties, creation of an email account, safety related tracking, protecting children from harmful content, and confirming age, each subject to certain conditions.¹⁶ Only sub-sections (1) and (3) of Section 9 are disapplied. Sections 6 and 8 and Section 9(2) continue to bind, so a fiduciary that relies on an exemption still owes duties of minimisation and security.

E. Commencement

The Rules come into force in various stages. Provisions regarding the Board and certain procedural matters took effect on publication. The consent manager provisions follow after twelve months. The core fiduciary obligations, Rule 10 among them, follow after eighteen months, which commentators calculate as falling around 13 May 2027.¹⁷ A proposal to shorten the eighteen-month period to twelve months has been reported, but trackers consulted for this paper record that it had not been notified as of September 2026.¹⁸ This timing explains the paper's method. The child-protection duties are not yet enforceable, so the analysis has to be predictive.

F. What the framework defines and what it leaves open

The Act and the Rules are precise about who must obtain consent (the fiduciary), from whom (the parent or lawful guardian), when (before processing) and how much is at stake (the penalty tier). They also name illustrative methods of verification.

They say far less about the *standard* to be met. Nowhere is there a definition of “verifiable” consent, of “tracking or behavioural monitoring” or “targeted advertising”, of how a fiduciary should decide that a user is a child, of “lawful guardian” in the case of minors, or of the well-being test in Section 9(2). Rule 10 gives tools without saying how much assurance is enough. That gap is the subject of Part IV.

III. LITERATURE REVIEW

A. Indian commentary on Section 9 and Rule 10

The most direct treatment of the operational problem comes from Novo Juris, writing on the draft Rules in early 2025. Its central warning is that Rule 10 may mandate fiduciaries to check the age of *every* user, since a fiduciary cannot seek parental consent until it has established that a user is a child. It adds that the draft appeared to bite only on users who declare themselves to be children or parents, and that self-declaration is an unreliable trigger. It also faults the undefined expression “reliable details”, observing that a parent’s registration record may amount to nothing more than an email address, and it points to the unclear method of proving the parent–child relationship. Its suggested remedy is to borrow from COPPA, namely an enumerated list of verification methods and a platform centred approach in which the strictest duties fall on child-directed services.¹⁹

Ikigai Law’s note turns to the *final* Rules. It reports that they closely track the draft, that the children’s data obligations start eighteen months after notification (13 May 2027), and that Rule 10 offers three verification routes: details the fiduciary already holds, details the parent volunteers, and tokens issued by government authorised entities. It also records two additions to the Fourth Schedule exemptions, namely real time location tracking for child safety and tracking needed to keep harmful content or advertising away from a child, and suggests that the latter may signal that some personalisation is permitted where it serves online safety.²⁰ That observation shows how much depends on terms the Act leaves undefined.

Tandon and Sharma concentrate on the *burden* that Section 9 places on families. In their account, parents face “identity verification fatigue”, having to prove who they are afresh for each service, and “consent fatigue”, having to read a separate notice each time. They propose a Common Consent Mechanism modelled on the approach the US Federal Trade Commission recognised under COPPA, in which an app store verifies a parent once and other apps rely such outcome, while each app keeps its own duty to obtain informed consent. They also argue that app stores would remain within the intermediary safe harbour in Section 79 of the Information Technology Act.²¹ The proposal would cut repeated verification, but it does not say what standard the single verification must satisfy.

Two further works locate India in the comparative landscape. A 2026 study in the *International Journal of Law Management & Humanities* presents Section 9 as India’s principal answer to children’s data risks and compares it with the GDPR and the Digital Services Act, with verifiable parental consent and age verification as recurring themes.²² A broader preprint,

“Local Privacy Laws in a Globalized World”, tabulates children’s age thresholds across jurisdictions: under 16 for the GDPR (lowerable to 13), under 13 for the CCPA, under 14 for China’s PIPL, under 12 for Brazil’s LGPD and under 18 for the DPDP Act.²³ These works establish how *high* India’s threshold is, but they are concerned with the level of the threshold, not with the way the duties are applied.

B. Age assurance, privacy and circumvention

The most rigorous analysis of the underlying technical problem is that of Lueks, Dreyer, Federrath and Simon, who assess age verification, age estimation, age inference and parental consent for effectiveness, side effects and acceptance.²⁴ Four of their findings bear directly on this paper:

- Every method can be circumvented, including by “adult by proxy”, where any adult, not necessarily a parent, completes the check on the child’s behalf.
- *Age inference*, which deduces age from behaviour, is highly invasive and offers low assurance, and it risks becoming a pretext for further data collection in place of minimisation.
- Under the GDPR and the Digital Services Act (DSA) there is an unresolved circularity: establishing age itself requires personal data, which may conflict with minimisation.
- Legislators should not rest on high-level principles such as data minimisation, because such principles admit both privacy-preserving and privacy-invasive implementations. They should instead specify concrete properties, like selective disclosure, unlinkability and no retention beyond the age attestation.

A practitioner article in the IAPP’s news service adds an empirical note. It reports research, led by an age verification industry body and therefore coming from an interested party, that most EU countries apply little or no age verification and that self-declaration predominates where verification exists.²⁵ Even a “reasonable efforts” standard, on this evidence, doesn’t guarantee a genuine verification unless it is given content.

C. Theory: rules, standards and the limits of consent

Three general works, none specific to India, frame the problem. Kaplow’s economic analysis separates the rules, which fix conduct in advance, from standards, which leave content to be supplied later.²⁶ Section 9 is a hybrid. Its penalties are fixed and severe, like a rule, while its key terms are open textured, like a standard, and no adjudicator or guidance has yet supplied

their content. Solove argues that consent based “privacy self management” cannot work at scale.²⁷ Waldman contends that procedural privacy compliance can degenerate into “compliance theatre”, in which firms perform the legal formalities without changing what they actually do.²⁸ Taken together, these accounts help explain why open textured consent duties can lead to both excessive and merely namesake compliance.

D. The gap

The works surveyed establish five points. India’s threshold is unusually high (Part III.A). Rule 10’s mechanics are unclear in places (NovoJuris). Repeated verification is burdensome for families (Tandon and Sharma). Age assurance methods carry expensive side effects and can always be circumvented (Lueks and others). And consent regimes move towards formalism (Solove; Waldman).

In the sources reviewed, none treats the *absence of definitions and standards* as a single structural cause of *two opposite* compliance failures, over collection and under compliance, within the DPDP framework. NovoJuris comes closest, since it identifies both symptoms (verifying every user, and the unreliability of self declaration) without framing them as one thesis. This paper builds that connection, tests it against the text of the Act and the Rules, and evaluates the GDPR’s risk proportionate model as a possible remedy.

IV. THE DEFINITIONAL GAP

A. The undefined terms

Table 1 collects the terms on which Section 9 and Rule 10 depend and records what the text leaves unanswered for each.

Table 1: Undefined or under specified terms in Section 9 and Rule 10

Term	Where it operates	Defined?	Main open questions
“Verifiable” consent	s 9(1); r 10	No definition; r 10 lists methods	What level of assurance is enough? Is one method sufficient?
Who is a “child” (age assurance)	s 9(1); r 10	s 2(f) fixes the age, not the test	Must a fiduciary know a user’s age, estimate it, or verify everyone?
“Parent” and “lawful guardian”	s 9(1); r 10	Not defined for minors	Which parent? How is the relationship shown? What of separated or absent parents?

“Tracking or behavioural monitoring”	s 9(3)	No	Do analytics, personalisation or recommendations count?
“Targeted advertising directed at children”	s 9(3)	No	Is contextual advertising excluded? What makes an advertisement “directed at” a child?
“Detrimental effects on well-being”	s 9(2)	No	Who decides, and on what evidence?
“Verifiably safe”	s 9(5)	No	What criteria will the Central Government apply?
“Appropriate technical and organisational measures”; “due diligence”	r 10	No	What counts as appropriate or sufficient diligence?

On the reading adopted here, none of these expressions is defined in Section 2 of the Act, and Rule 2 adds only a definition of “user account” and related terms.²⁹

B. Verifiable consent: methods without a standard

Rule 10 is the most detailed provision on point. It requires a fiduciary to adopt appropriate technical and organisational measures and to exercise due diligence that the person claiming to be a parent is an identifiable adult. It then describes the routes to verification: reliable identity and age details already kept, details voluntarily supplied, or a virtual token issued by an authorised entity.³⁰

That is a list of *tools*, however, not a *standard*. The Rule does not lay how much assurance a fiduciary must reach, whether one route suffices for every service, or whether a low risk service may verify less than a high risk one. Commentators criticised the draft Rules on exactly this ground, pointing out that “reliable details” was left undefined and that information a parent supplied at registration, often only an email address, may be inaccurate or false.³¹ The final Rules retain the tool based approach. A fiduciary can therefore satisfy the wording of Rule 10 while remaining unsure whether it has satisfied the Rule’s purpose.

C. Identifying a child: the circular trigger

Section 9(1) applies “before processing” a child’s data, which presupposes that the fiduciary already knows the user is a child. Yet neither the Act nor the Rules say *how* it is to know. Three readings are open: actual knowledge only, a duty to take reasonable steps to find out, or a duty to verify the age of every user. The text does not choose between them, and the choice is far from minor, because it decides whether a fiduciary must collect age data from all users or need act only when a child identifies as one. Part V shows how the cautious reading leads to over-collection, and Part VI how the lenient reading leads to under-compliance.

D. Parent and lawful guardian

Rule 10 speaks of a person “identifying herself as the parent” and requires the fiduciary to check that she is an identifiable adult. The Rule’s illustrations show how the check works depending on whether the parent is already a user of the platform.³² What remains open is the *relationship*. Must the fiduciary confirm that this adult is this child’s parent and, if so, by what documents? Which parent must consent where the parents disagree or live apart? What of children with no parent available, such as those in institutional care? For persons with disabilities, Rule 11 relies on a “lawful guardian”, but for minors the Act does not say who else qualifies. A fiduciary may lean towards demanding proof of the relationship, which is intrusive, or towards accepting any adult, which is weak.

E. Behavioural monitoring and targeted advertising

Section 9(3) names three activities, “tracking”, “behavioural monitoring” and “targeted advertising”, and defines none of them. The Rules offer two hints. The Fourth Schedule exempts, under certain conditions, purposes such as safety tracking, shielding children from harmful content and age confirmation.³³ The existence of these carve-outs suggests that “tracking” is meant to be read broadly, since narrower reading would make them unnecessary. That is only an interpretive inference, however, and it does not tell a fiduciary where the line falls between prohibited monitoring and ordinary product functions such as analytics, fraud detection, personalised recommendations or contextual advertising. Commentators have also noted that the exemption structure was presented as a way of enabling a risk-based approach, although no test for what counts as risky was supplied.³⁴

F. The well-being test and the “verifiably safe” route

Section 9(2) forbids processing likely to harm a child’s well-being but offers no criteria, no

process for assessment and no examples. Section 9(5) permits a lower age threshold for fiduciaries whose processing is “verifiably safe”, again without saying what evidence or standard the Central Government will apply. Both provisions look like flexible, risk sensitive tools. Empty of content, though, they give fiduciaries no basis for planning, and so they cannot be relied on either to design services or to seek the exemption.

G. The consequence: high penalties on undefined duties

These gaps matter because they sit under a larger enforcement regime. Failure to meet the children’s data obligations attracts one of the highest penalty tiers in the Schedule.³⁵ Attaching bigger monetary penalties to duties whose boundaries are unclear raises a legal certainty concern. Indian courts have treated vagueness as a serious defect in other settings. In *Shreya Singhal v Union of India*, the Supreme Court struck down section 66A of the Information Technology Act largely because its terms were too vague to give fair notice.³⁶ The analogy is imperfect, because that case concerned a criminal restriction on speech whereas this paper concerns civil penalties. It nevertheless supports the general proposition that those exposed to liability are entitled to know what conduct is required of them.

H. Bridge to Parts V and VI

The gap does not produce a single response. A fiduciary unsure what “verifiable” or “monitoring” means can protect itself in two opposite ways. It can do *more* than what the law requires, collecting identity and behavioural data to demonstrate diligence. Or it can do *less*, adopting the thinnest reading the text will bear. Part V takes the first response and Part VI the second.

V. OVER-COLLECTION: THE CAUTIOUS RESPONSE

A. The incentive to over shoot

Part IV showed that Section 9 and Rule 10 hand fiduciaries tools without a standard. This Part asks what a rational, risk-averse fiduciary does in that position. The answer starts with an asymmetry in the cost of error. A fiduciary that verifies too little risks a Board inquiry and a penalty of up to ₹200 crore for children’s-data failures.³⁷ A fiduciary that verifies too much bears friction, engineering cost and some lost users, but faces no sanction that is comparably certain or comparably prominent. Because “verifiable” has no threshold, the fiduciary cannot know when it has done enough. The only way to be sure is to do more than enough.

Kaplow's differentiation between rules and standards helps explain the mechanism.³⁸ Section 9 pairs a standard-like duty (verifiable consent, no monitoring) with a rule-like penalty. When a vague standard carries a large fixed sanction, a risk-averse actor protects itself by over-complying, because the cost of misjudging the standard's content falls entirely on the actor, while none of the cost of excess falls on the regulator.

A second pressure arises where two open textured duties collide. The fiduciary must verify enough to satisfy Section 9(1) and Rule 10, yet must also collect only what is actually necessary under Section 6(1). In principle the second limits the first. In practice the two are unlikely to be enforced with equal force. The harm from under-verification is a visible child. The harm from over collection is diffuse, falls on adults who are unlikely to complain, and engages a very different and less prominent penalty tier.³⁹ The prediction is therefore that minimisation will give way to the more salient duty. This is a structural prediction about incentives, not a claim about the intentions of any firm.

B. Three channels of over collection

1. **Universal age assurance.** Part IV.C identified three readings of how a fiduciary comes to know that a user is a child: actual knowledge, reasonable steps, or verification of everyone. Only the third leaves no room for error, and a cautious fiduciary will drift towards it. Once it does, every user, adults included, must give age data or an age credential before the service begins. A regime meant to protect children then imposes a data cost on the whole user base.

The age data is itself new personal data, carrying its own security and erasure duties under Section 8.⁴⁰

2. **Documentary verification of the parent and of the relationship.** Rule 10 requires due diligence that the consenting person is an identifiable adult and offers, as one route, a virtual token issued by an authorised entity, including through Digital Locker services.⁴¹ Faced with an open standard, a fiduciary will tend to choose the artefact that is easiest to defend in an inquiry, namely a government-issued identifier, over the one that is least intrusive. The tendency is stronger for the unresolved question of the parent-child relationship (Part IV.D). A fiduciary anxious to prove that this adult is this child's parent may ask for birth certificates, school records or guardianship papers. Each request adds sensitive data, links the child's account to a real-world parental identity, and concentrates material in a database that is an attractive target for attackers. Nothing in Rule 10, as read here, requires the fiduciary to accept only a yes or no attestation or

to delete verification records once the check is done.⁴²

3. **Age inference through profiling: the verification paradox.** A fiduciary wishing to avoid document requests may try to work out who is a child from behaviour, such as content viewed, hours of use, typing patterns, contacts or device signals, or from facial or voice estimation. This is the most troubling channel, because it turns the compliance measure into the prohibited activity. Section 9(3) forbids tracking and behavioural monitoring of children, yet to identify children by their behaviour the fiduciary must first track and analyse the behaviour of everyone, children included. Its only defence is the age-confirmation purpose in Part B of the Fourth Schedule, whose conditions and reach must be tested against the final text.⁴³ This paper terms the resulting loop the *verification paradox*: to prove that it does not monitor children, the fiduciary monitors all users. Lueks and colleagues report the same risk. Age inference is highly invasive, gives low assurance and can become an excuse for further data collection instead of minimisation (Part III.B). The GDPR and DSA settings display the same circularity, since determining age itself requires personal data.

C. What the cautious response costs

Four costs follow. First, adult users lose privacy to a duty that was meant to protect someone else. Second, exclusion: a family without a ready identity credential, with limited digital literacy, or with a single shared phone may be unable to complete verification, so that the child loses access to services that are educational or otherwise beneficial. The scale of this effect is an empirical question that cannot be answered until the duties commence, and this paper makes no claim about its size. Third, security: verification data creates a concentrated store of identity material, which brings in the Section 8 safeguard duty and enlarges the consequences of any breach. Fourth, function creep: data collected to establish the age is easily repurposed for analytics or advertising unless law forbids it, and the Act's purpose limitation works only through the notice and consent given for the original purpose.

D. Illustrations

The scenarios below are hypotheticals created for this paper. They do not describe any real service, and they show only what the drafting makes rational.

Illustration A (education). A private test preparation app serves pupils in classes 9 to 12 and is paid for by parents. To be safe, it requires every parent to complete a Digital Locker token check and to upload the child's school identity card, and it keeps the copies "for audit". It is

unsure whether a commercial app counts as an “educational institution” under Part A of the Fourth Schedule, and so assumes that it does not.

Illustration B (gaming). An online multiplayer game with voice chat has players aged between ten and twenty. To identify minors, it demands a selfie based age estimate at sign up for every new account, analyses voice samples in chat to flag young speakers, and retains the biometric templates for periodic re verification.

Illustration C (social media). A short-video platform verifies all users with a government identifier and, separately, scores every account for likely age using watch behaviour, contact graphs and device signals. Accounts that score as probable children are routed into a parental-consent flow.

In each case the fiduciary’s conduct is intelligible. In each case, too, it collects more than a narrow reading of the purpose would require, and in Illustrations B and C it engages in the very kind of behavioural analysis that Section 9(3) targets.

E. Assessment

The over-collecting fiduciary is not acting in bad faith and, on the face of Rule 10, is not clearly in breach, since the Rule lists these tools. Its conduct nonetheless sits uneasily with the necessity limit in Section 6(1) and with the minimisation principle that limit expresses. The fault lies in the missing standards, not in the firm. Without a statement of how much assurance is enough for which kind of service, a fiduciary cannot tell where diligence ends and excess begins. This is the first half of the dual-failure thesis. The second half, under-compliance, arises from the same uncertainty and is examined next.

VI. UNDER-COMPLIANCE: THE CEREMONIAL RESPONSE

A. The incentive to under-shoot

The uncertainty that makes a cautious fiduciary towards excess makes a less cautious one the other way. Four features of its position make the thinnest reading attractive. First, there is no adjudicated interpretation yet, so a fiduciary can plead good faith reliance on the plain words of the text. Second, friction shows up at once in conversion rates, whereas the harm of thin protection is diffuse and appears on no dashboard. Third, business models built on engagement and personalisation depend on exactly the behavioural data that Section 9(3) restricts. Fourth, enforcement is largely reactive: as drafted, the Board’s inquiry powers are set off by complaints, intimations of breach and references, and children rarely complain.⁴⁴ The

likelihood of detection is therefore modest, at least until practice develops.

Waldman's account of "compliance theatre" describes the outcome: firms carry out visible steps the law seems to order while leaving underlying practice untouched.⁴⁵ Solove's critique of consent-based privacy self-management adds that once a consent click is obtained it is treated as the end of the matter.⁴⁶

B. Five forms of under-compliance

1. **Self-declaration and engineered ignorance.** Commentators observe that Rule 10 appears to apply only where a user identifies as a child or as a parent (Part III.A). A fiduciary can then design its onboarding so that users never identify as children, for instance through a date-of-birth field that accepts any adult date or an "I am 18 or over" checkbox. This is the actual-knowledge reading of Part IV.C pushed to its limit, and it rewards wilful blindness. COPPA, which ties its duties partly to actual knowledge, meets the same criticism (Part VII.D).
2. **Adult by proxy.** Rule 10 requires an "identifiable adult", not a demonstrated parent. A phone number or email address of unknown ownership, confirmed by a one-time code, may satisfy the wording. The child then completes the flow with an older sibling's number, a friend's, or a second SIM of their own. Lueks and colleagues list this "adult by proxy" circumvention as a weakness of every verification method, and the Rule's reference to "reliable details" that may be no more than an email address makes it easier still.
3. **Definitional narrowing.** Because "tracking", "behavioural monitoring" and "targeted advertising" are undefined, each can be re-labelled. Behavioural advertising becomes "personalisation" or "recommendations", and profiling becomes "product analytics". The drafting of Section 9(3) supplies a textual hook: the phrase "directed at children" attaches to advertising, so a general-audience platform can argue that its advertising is not directed at children at all, while "of children" attached to tracking and monitoring can be read to require that the fiduciary know who the children are. The Fourth Schedule exemptions invite similar treatment. Ikigai Law notes that the harmful-content exemption may recognise a degree of permitted personalisation (Part III.A), and a fiduciary can stretch that recognition into a general licence to track.
4. **Exemption shopping.** A fiduciary that can plausibly describe itself as an educational institution, a healthcare provider or a child-care service may claim the Part A class exemption and escape Sections 9(1) and 9(3) altogether. The boundaries of those classes

are undefined for commercial services that operate close to them, as Illustration A shows. Section 9(2), the well-being test, survives such an exemption, but it too is undefined (Part IV.F).

5. **One-time, ceremonial consent.** Where verification is a single click at sign-up, consent becomes a gate passed once and never revisited. Tandon and Sharma's "consent fatigue" describes the parent's side of the same problem: a parent asked for approval by many services will approve without reading.

C. The flat threshold amplifies evasion

India's flat age of eighteen (Section 2(f)) enlarges the population that must be treated as children, and the added group consists mostly of older teenagers. Full verifiable parental consent for a seventeen-year-old is a heavy burden relative to the risks, and it gives a parent oversight of the online life of a young adult who may reasonably want privacy, for example when seeking health information or counselling. The UN Committee on the Rights of the Child, in General Comment No 25, stresses the evolving capacities of the child in the digital environment.⁴⁷ A rule that treats a seventeen-year-old like a seven-year-old gives both the fiduciary and the teenager a reason to evade it. Over-inclusion in the threshold thus feeds the under-compliance channels above. The point complements the comparison in Part VII, since the GDPR and COPPA both set the consent line far below eighteen.

D. One fiduciary, both failures

The dual-failure thesis does not require that some firms over-collect while others under-comply. A single fiduciary can do both. Rule 10 measures an act, the verification of the parent, and not an outcome, the absence of monitoring inside the product. A fiduciary can therefore build a demanding gate at the entrance and leave the product behind it largely unchanged. Verification is measured at the door, and protection inside is unmeasured. Illustration C, extended, shows the pattern: strong identity checks at registration, followed by an engagement driven recommendation engine that treats every account alike.

E. The illustrations revisited

Table 2 sets each hypothetical fiduciary from Part V beside a less cautious counterpart.

Table 2: Over-collecting and under-complying responses to the same scenarios

Illustration	Over-collecting response (Part V)	Under-complying response (this Part)	What the text leaves unresolved
A. Test-prep app	Identity token and school ID for every family; copies retained.	Claims to be an “educational institution” under Part A of the Fourth Schedule; parental tick-box; behavioural analytics to upsell continue.	Whether a commercial edtech service falls within Part A; what “verifiable” requires.
B. Multiplayer game	Selfie age estimate and voice analysis for all players; biometric templates retained.	Date-of-birth gate that blocks under-18s in name only; in-game purchase prompts tailored to play behaviour, labelled “personalisation”.	Whether tailored purchase prompts are “targeted advertising”; whether age estimation is itself monitoring.
C. Short-video platform	Government ID for all users plus behavioural age scoring.	Self-declared 18+ gate; “general audience” claim; engagement-based recommendations justified as harmful-content safety.	Whether a general-audience service must look for children; scope of the harmful-content exemption.

Each response is rational on the present text. Neither is what the section was created to achieve, and neither corrects itself: the over-collector is not penalised for excess, and the under-complier goes undetected until a complaint arrives. The same missing standard explains both.

VII. THE COMPARATIVE MODEL: RISK-PROPORTIONALITY AND ITS LIMITS

This Part does not recommend a straight forward transplant. Its aim is to see how other regimes give content to open standards like those in Section 9, and to test the claim made in the abstract that a risk-proportionate approach offers India a way out of the dual failure. The argument is that it does, but only in part.

A. The GDPR: Articles 5, 8 and 25

Article 8 GDPR sets the age of digital consent at sixteen, leaving Member States free to lower it, though not below thirteen. Its reach is narrower than that of Section 9, because it applies only where consent is the lawful basis and the service is an information society service offered directly to a child.⁴⁸ Other bases in Article 6, including contract and legitimate interests, remain available, and Article 6(1)(f) orders particular care where the data subject is a child. Section 9(1), by contrast, is framed as a duty that attaches before *any* processing of a child's personal data. Whether it displaces the legitimate uses recognised in Section 7 is a question this paper does not resolve.⁴⁹

Article 8(2) is the provision closest to the Rule 10 problem. It requires the controller to make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility, taking available technology into consideration. That is a proportionality clause: the effort demanded rises and falls with the risk and with what technology makes reasonable. The surrounding architecture supports it. Article 5(1)(c) states the minimisation principle, Article 5(2) makes the controller accountable for demonstrating compliance, Article 25 needs data protection by design and by default, and Article 35 asks for an impact assessment where processing is likely to result in high risk. Together these ask the controller to assess risk, document the reasoning and choose measures accordingly, under the oversight of supervisory authorities that issue guidance. The European Data Protection Board's statement on age assurance, adopted in February 2025, is an example. It treats age assurance as a risk related exercise constrained by minimisation.⁵⁰

The GDPR is nonetheless not a complete answer. Article 8(2) is itself vague. The IAPP reports, on the strength of industry-led research, that verification in practice is thin and largely self-declared (Part III.B), and Lueks and colleagues identify the unresolved circularity between establishing age and minimising data. What the GDPR demonstrates is a method, namely proportionality combined with accountability and guidance. It does not show that the method works without the guidance.

B. The UK Age Appropriate Design Code

The UK Code is the most instructive comparator for India, because it applies to children under eighteen, as Section 2(f) does, while pairing that threshold with graduated, design-based duties. It reaches services "likely to be accessed by children", a scope test with content that Section 9 lacks. Its standard on age-appropriate application gives the service provider a choice: establish the age of users with a level of certainty appropriate to the risks of the processing, or apply the

Code's protections to all users.⁵¹ The second option dissolves the circular trigger of Part IV.C, because a service that gives every user child-appropriate defaults need not identify who the children are. Other standards address what Sections 9(2) and 9(3) leave open: profiling is to be off by default, data may not be used in ways detrimental to children's well-being, and collection is to be minimised. The Code has statutory backing, and the Information Commissioner's Office has enforced the underlying consent requirements, including a £12.7 million monetary penalty announced in April 2023 against a video-sharing platform for processing the data of under-thirteens without parental consent.⁵² Enforcement of this kind supplies the missing content case by case, but it also shows how long the process can take.

C. The Digital Services Act: Article 28

Article 28 of the DSA contains three provisions that speak directly to the dual failure. Paragraph 1 requires online platforms which are accessible to minors to adopt appropriate and proportionate measures to ensure a high level of privacy, safety and security. Paragraph 2 bars advertising based on profiling where the provider is aware with reasonable certainty that the recipient is a minor. Paragraph 3 provides that these duties do not oblige providers to process additional personal data in order to assess whether a user is a minor.⁵³ The last of these is an express legislative answer to the verification paradox. The "awareness with reasonable certainty test" also answers a question that Section 9 leaves silent, namely how a fiduciary is to know that a user is a child. It is a knowledge standard with content, sitting between the actual-knowledge and verify-everyone readings.

The Commission's guidelines of July 2025 explain what "proportionate" means in practice. They recommend age assurance that is accurate, reliable, robust, non-intrusive and non-discriminatory, and they prefer verification for high-risk uses such as adult content and gambling, with lighter measures elsewhere.⁵⁴ The guidelines are not binding, but the Commission treats them as a benchmark for assessing compliance. They have also attracted criticism from scholars who argue that they overstate the proportionality of age verification and estimation and give too little weight to data protection.⁵⁵

D. COPPA

The United States Children's Online Privacy Protection Act draws its line at thirteen and imposes its strictest duties on operators of child-directed services and on operators with actual knowledge that they are collecting data from a child.⁵⁶ Its regulations do what India's Rules do not. They define "directed to children" through a multi-factor test, list approved methods of

verifiable parental consent, and allow operators to seek Federal Trade Commission approval of new methods, while approved industry self-regulatory programmes provide a safe harbour. The list of methods scales to risk in one respect, since a lighter method, commonly called “email plus”, is permitted where data is used only internally.

The lessons cut both ways. COPPA supplies certainty, which is precisely what Section 9 lacks, and it is the model NovoJuris suggests borrowing (Part III.A). But its actual knowledge trigger brings in the engineered ignorance described in Part VI.B, and its narrow age band leaves teenagers largely outside. An enumerated list of methods without a risk gradient could also entrench the over-collection channel, since the most robust items on such lists tend to be identity-heavy. Borrowing COPPA’s certainty without its weaknesses calls for the additional safeguards discussed in Part VIII.

E. Side-by-side comparison

Table 3 summarises the five regimes on the dimensions that matter most for the dual-failure argument. It is a simplified summary and is not a substitute for the primary texts.

Table 3: Comparative summary of the five regimes

	India (DPDP Act and Rules)	GDPR	UK Code	EU DSA, art 28	US COPPA
Age threshold	18, flat (s 2(f))	16, lowerable to 13 (art 8)	Under 18 (Code); 13 for consent	Minors (under 18)	Under 13
Trigger for duty	Undefined: how a child is identified is not stated	Consent basis; service offered directly to a child	Service likely to be accessed by children	Platform aware with reasonable certainty (art 28(2))	Child-directed service or actual knowledge
Verification standard	Methods listed in r 10; no level of assurance	Reasonable efforts, given available technology (art 8(2))	Certainty appropriate to risk, or apply to all users	Appropriate and proportionate; Commission guidelines	Enumerated methods; FTC approval route

Limit on monitoring and profiling	s 9(3): undefined terms; exemptions	Principles (arts 5, 25); profiling limits	Profiling off by default; detrimental-use standard	No profiling-based ads to known minors	Conditions on collection; targeted-ad limits vary
Safeguard against over-collection	s 6(1) necessity; nothing specific to age data	Minimisation (art 5(1)(c)); DPIA (art 35)	Data minimisation standard	Express: no additional data needed to assess age (art 28(3))	Data minimisation and retention rules
Interpretive infrastructure	Board not yet operating on children's data; no guidance	Supervisory guidance; EDPB statements	Statutory code; ICO enforcement	Commission guidelines (non-binding benchmark)	Detailed rule; safe harbours; FTC approvals

F. What travels and what does not

Four features of the Indian setting affect how far these models can be transplanted.

First, India has public digital infrastructure, including Digital Locker and consent manager frameworks, that could make privacy preserving verification practical: a token stating only that the holder is an adult, or that a named adult is linked to a child, and nothing more. The same infrastructure creates a risk that fiduciaries will default to state identity documents simply because they are available. Rule 10's reference to tokens issued by authorised entities is a starting point, but the Rule does not say what such a token may reveal.

Second, regulatory capacity differs. The GDPR's reliance on open standards works because mature supervisory authorities give guidance and enforce. India's Board is newly constituted, and the children's data duties have not yet commenced. This weakens the case for copying the GDPR's open texture and strengthens the case for stating concrete content in the Rules or in binding guidance. Lueks and colleagues reach a parallel conclusion: high level principles such as minimisation allow both privacy preserving and privacy invasive implementations, so legislators should specify properties such as selective disclosure, unlinkability and no retention beyond the attestation.

Third, the flat threshold is set by statute. Section 2(f) cannot be tiered by Rules. The tools available are the exemptions under Section 9(4) and the age lowering notifications for verifiably safe processing under Section 9(5). A truly graduated regime for older teenagers would need an amendment.

Fourth, the constitutional background favours a proportionate reading. In *Puttaswamy* the Supreme Court recognised privacy as a fundamental right and required that the restrictions be proportionate, and the later Aadhaar decision applied the proportionality test in that context.⁵⁷ Those cases concern State action, whereas Section 9 regulates private fiduciaries, yet they support reading a child protection duty in a way that does not demand not a proportionate identity disclosure. Together with *Shreya Singhal* (Part IV.G), they support the view that those subject to liability are entitled to clear standards.

The refined conclusion is this. A risk proportionate approach can break the dual failure, but only when it is paired with concrete properties and guidance. The GDPR's own experience reveals proportionality without content produces thin compliance. India's need for explicit content is greater, not smaller, than Europe's.

VIII. RECOMMENDATIONS

The recommendations follow from the analysis. They aim to give the open terms of Section 9 enough content to guide conduct without freezing technology, and to steer fiduciaries away from both failures at once. They are addressed to the actors with legal power to act: the Ministry of Electronics and Information Technology (MeitY), through the Rules or notifications; the Data Protection Board, through guidance and enforcement practice; and, where relevant, fiduciaries themselves. Timing matters. The core obligations are expected to apply from around 13 May 2027. A proposal to shorten the period to twelve months, which would bring the date forward to 13 November 2026, was reported after a January 2026 consultation, and trackers consulted for this paper record that no notification had been made as of September 2026.⁵⁸ In either case, guidance should come before commencement. Table 4 links each problem identified in the paper to a proposed remedy and the actor responsible.

Table 4: Problems identified and proposed remedies

Problem (Part)	Recommendation	Actor and instrument
No standard of “verifiable” (IV.B, V)	Adopt risk-tiered assurance levels (low, medium, high) with example mappings to service types; a low-risk service may verify by a lighter method.	MeitY (Rules amendment); Board (guidance)

Circular trigger (IV.C, V, VI)	State a knowledge standard: actual knowledge, or knowledge reasonably inferable for general-audience services, together with a “likely to be accessed by children” test for services aimed at or attractive to children. Provide that no service must verify all users solely to comply with s 9.	MeitY (Rules amendment)
Over-collection and the verification paradox (V)	Require privacy-preserving properties: age or relationship attestations that disclose no more than the fact needed (selective disclosure), no linking across services, no retention beyond the attestation, and no reuse of age data for other purposes. Prohibit behavioural age inference except where strictly permitted.	MeitY (Rules); Board (guidance)
Undefined monitoring and advertising (IV.E, VI)	Publish illustrative guidance separating prohibited behavioural monitoring and targeted advertising from permitted functions such as security, fraud prevention, aggregate analytics and contextual advertising. Set out factors for “directed at children” (subject matter, audience composition, child-oriented design).	Board (guidance); MeitY (Rules)
“Parent” and “lawful guardian” (IV.D)	Treat consent by either parent as sufficient unless the fiduciary has notice of a dispute; provide fallback guardians (for example, institutional carers) for children without a parent; draw on existing guardianship law for content.	MeitY (Rules); Board (guidance)
Flat threshold and teen evasion (VI.C)	Use ss 9(4) and 9(5) to build a graduated regime: lighter verification and protective defaults for older teenagers, stricter measures for younger children; consider amending s 2(f) in the longer term.	MeitY (notification); Parliament (amendment)

Ceremonial consent and exemption shopping (VI)	Clarify the scope of the Part A classes for commercial services; require periodic reconfirmation of parental controls for high-risk services.	MeitY (Rules); Board (guidance)
Penalty on undefined duties (IV.G, VI)	Recognise good-faith compliance with Board-approved methods as a mitigating factor under s 33(2) and encourage voluntary undertakings under s 32; publish enforcement priorities.	Board (practice and guidance)
Repeated verification (III.A)	Permit a shared verification mechanism, for example at operating-system or app-store level, with each service retaining its own consent duty; guard against gatekeeper concentration.	MeitY; Board; industry

A. The core recommendation: a risk-tiered standard of assurance

The most important step is to replace “methods without a standard” with a proper graded standard. A low risk service, such as a reference tool that collects almost no data, should be able to rely on a lighter method. A service that profiles users, enables contact between strangers or sells to minors should be held to a higher level of assurance. This follows the idea of GDPR Article 8(2) and the DSA guidelines, and it borrows COPPA’s certainty by naming the accepted methods at each level. A graded standard addresses both failures: it tells the cautious fiduciary when it may stop, and it tells the lenient fiduciary when a checkbox is not good enough. To prevent the enumerated methods from establishing identity heavy verification, each level should also state the properties described next.

B. Concrete privacy properties

Following Lucks and colleagues, the Rules or binding guidance should specify properties instead of depending on the general principle of minimisation. Those properties are selective disclosure (a token that says only that the holder is an adult, or that an adult is linked to a child), unlinkability (different services cannot correlate the same person) and deletion of verification records once the attestation is made. A rule that age data may be used only for age assurance, together with an express statement in the style of DSA Article 28(3) that no fiduciary is obliged to process additional personal data merely to determine age, would close the verification paradox. Age inference by behavioural profiling should be permitted only where it is strictly

necessary and is the least intrusive means available.

C. Definitions through guidance, not only through Rules

Definitions of tracking, behavioural monitoring and targeted advertising should be developed through illustrative Board guidance, because technology and business practice will change faster than the Rules can. Guidance can carry examples, safe and unsafe, that a definition cannot. The list of exemptions in the Fourth Schedule shows that the drafters expected such line-drawing, and the same guidance should say how far the harmful-content and safety-tracking exemptions extend.

D. Teenagers and the flat threshold

Section 9(5) allows the Central Government to notify a lower age for fiduciaries whose processing is verifiably safe. The Government should publish the criteria for that finding. Doing so would give fiduciaries something to design towards and would lessen the incentive for teenagers and fiduciaries to evade a rule that fits older teenagers badly. In the longer term Parliament should consider whether a graduated threshold better serves the purposes of the Act, which would also be consistent with the evolving-capacities principle in General Comment No 25.

E. Enforcement calibrated to good faith

The Board's enforcement practice can reduce both failures. Section 33(2) directs the Board to consider factors such as the nature and gravity of the breach, mitigation and the proportionality of the penalty, and Section 32 allows voluntary undertakings.⁵⁹ If the Board signals that a fiduciary using an approved, privacy-preserving method will be treated as having acted in good faith, cautious fiduciaries lose the incentive to over-collect. If it also signals that ceremonial measures will not discharge the duty, the incentive to under-comply falls. Early enforcement should give priority to conduct that harms children in substance, meaning profiling and behavioural advertising aimed at them, over technical failures in verification flows.

IX. CONCLUSION

This paper set out to examine how the undefined terms in Section 9 of the DPDP Act and Rule 10 of the DPDP Rules, 2025 shape the behaviour of Data Fiduciaries. On the first research question, Part IV identified a cluster of undefined or under-specified terms: verifiable consent,

the test for identifying a child, parent and lawful guardian, tracking or behavioural monitoring, targeted advertising, the well-being test, verifiably safe processing, and the due-diligence standard in Rule 10. Rule 10 lists tools but does not state how much assurance is enough.

On the second question, Part V argued that the combination of a heavy penalty and an open standard gives a cautious fiduciary reason to over-collect: to verify every user, to demand identity documents and to infer age by profiling. The last of these creates a verification paradox, since to show that it does not monitor children the fiduciary must monitor everyone. On the third question, Part VI argued that the same uncertainty allows a less cautious fiduciary to meet the wording of the law through self declaration, adult by proxy consent, re labelled tracking and one time clicks, and that the flat threshold of eighteen amplifies this tendency. The two failures share one cause, and a single fiduciary can commit both by verifying at the door and monitoring inside.

The comparative analysis in Part VII qualified the abstract's claim about the GDPR. Risk proportionate verification, data protection by design and the UK and DSA models offer real solutions, including the option of applying child appropriate protections to all users and the express rule that assessing age does not require additional data. Yet the GDPR's own proportionality clause is thin without guidance, and India's institutions are younger. The remedy is therefore proportionality supplied with content: risk tiered assurance levels, concrete privacy properties, a stated knowledge standard, guidance on monitoring and advertising, and enforcement that rewards good faith compliance (Part VIII).

Limitations and further research

Three limitations should be acknowledged. First, the argument is structural and predictive. The core obligations have not commenced, so no compliance behaviour has been observed, and the illustrations are hypotheticals. Second, the analysis is doctrinal and comparative and does not test the incentives empirically. Third, the description of the regimes outside India is necessarily selective, and several of them are changing. Once the obligations apply, empirical work should examine which verification methods fiduciaries adopt, what data they retain, how far self declaration predominates, how families without identity credentials fare, and how the Board interprets the open terms. Such work would show whether the dual-failure thesis is borne out in practice.

BIBLIOGRAPHY

A. Legislation and subordinate legislation

Children's Online Privacy Protection Act, 15 USC 6501–6506 (United States). Data Protection Act 2018 (United Kingdom), s 123.

Digital Personal Data Protection Act 2023 (India). Digital Personal Data Protection Rules 2025 (India). Information Technology Act 2000 (India), s 79.

Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1. Regulation (EU) 2022/2065 (Digital Services Act) [2022] OJ L277/1.

Children's Online Privacy Rule, 16 CFR Part 312 (United States).

B. Cases

Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

Justice K S Puttaswamy (Retd) v Union of India (2019) 1 SCC 1 (Aadhaar).

Shreya Singhal v Union of India (2015) 5 SCC 1.

C. Books, articles and preprints

Kaplow L, "Rules Versus Standards: An Economic Analysis" (1992) 42 Duke LJ 557.

Lueks W, Dreyer S, Federrath H and Simon J, "Assessing Age Assurance Technologies: Effectiveness, Side-Effects, and Acceptance" (arXiv:2603.25695, 26 March 2026) <https://arxiv.org/pdf/2603.25695>.

"Local Privacy Laws in a Globalized World" arXiv:2605.27801 <https://arxiv.org/pdf/2605.27801> [authors to be added].

"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" (2026) 9(3) IJLMH 4117 [author name to be added].

Solove DJ, "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126 Harvard Law Review 1880.

Tandon N and Sharma M, "The Curious Case of Common Consent: Rethinking Verifiable Parental Consent Under the DPDPA, 2023" (*Law School Policy Review*, 4 December 2025).

Waldman AE, "Privacy Law's False Promise" (2020) 97 Washington University Law Review 773.

D. Official guidance and international instruments

European Commission, Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(1) of Regulation (EU) 2022/2065 (14 July 2025).

European Data Protection Board, Statement 1/2025 on Age Assurance (February 2025).

Information Commissioner's Office, *Age appropriate design: a code of practice for online services* (2020). Information Commissioner's Office, monetary penalty notice against TikTok (April 2023).

UN Committee on the Rights of the Child, General Comment No 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25.

E. Commentary and online sources

Chambers and Partners, "MeitY plans to cut short DPDP Compliance Timeline and Notify Cross Border Restrictions for SDFs" (22 February 2026).

DPDP Rules tracker, <https://dpdpa.dcomply.in/rules/> (accessed September 2026).

DSA Observatory, "The Commission's approach to age assurance: Do the DSA Guidelines on protecting minors online strike the right balance?" (31 July 2025) [author name to be added].

IAPP, "Age verification and data protection: Far more difficult than it looks" (2026) [author and date to be added].

Ikigai Law, "A Closer Look at the DPDP Rules 2025" (14 November 2025).

MediaNama, "DPDP Rules: Platforms need parental consent to use children's data" (10 January 2025). NovoJuris, "Child's Personal Data and Privacy: Analysing the Draft DPDP Rules, 2025" (4 February 2025).

¹ Digital Personal Data Protection Act 2023, s 9.

² DPDP Act 2023, s 2(f).

³ Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, art 8.

⁴ Digital Personal Data Protection Rules 2025, r 10.

⁵ DPDP Rules 2025, r 1 (commencement). The date of 13 May 2027 is derived by counting eighteen months from notification; see Part II.E.

⁶ DPDP Act 2023, s 2(f).

⁷ DPDP Act 2023, s 5.

⁸ DPDP Act 2023, s 6(1).

⁹ DPDP Act 2023, s 8.

¹⁰ DPDP Act 2023, s 9(1)–(5).

¹¹ DPDP Act 2023, s 33 and the Schedule.

¹² DPDP Act 2023, Schedule (entry on additional obligations in relation to children under s 9).

¹³ Digital Personal Data Protection Rules 2025 (notified November 2025) [Gazette notification number to be added].

- ¹⁴ DPDP Rules 2025, r 10.
- ¹⁵ DPDP Rules 2025, r 10 (methods of verification).
- ¹⁶ DPDP Rules 2025, r 12 and Fourth Schedule, Parts A and B.
- ¹⁷ DPDP Rules 2025, r 1. The May 2027 date is a computed date and is reported as such by commentators, for example Ikigai Law, “A Closer Look at the DPDP Rules 2025” (14 November 2025) <https://www.ikigailaw.com/article/647/a-closer-look-at-the-dpdp-rules-2025>.
- ¹⁸ Chambers and Partners, “MeitY plans to cut short DPDP Compliance Timeline and Notify Cross Border Restrictions for SDFs” (22 February 2026) <https://chambers.com/articles/meity-plans-to-cut-short-dpdp-compliance-timeline-and-notify-cross-border-restrictions-for-sdfs>; DPDP Rules tracker <https://dpdp.dcomply.in/rules/> (accessed September 2026). Both are secondary sources.
- ¹⁹ NovoJuris, “Child’s Personal Data and Privacy: Analysing the Draft DPDP Rules, 2025” (4 February 2025) <https://www.novojuris.com/thought-leadership/child-s-personal-data-and-privacy-analysing-the-draft-dpdp-rules-2025.html>.
- ²⁰ Ikigai Law, “A Closer Look at the DPDP Rules 2025” (14 November 2025) <https://www.ikigailaw.com/article/647/a-closer-look-at-the-dpdp-rules-2025>.
- ²¹ Nandini Tandon and Mehul Sharma, “The Curious Case of Common Consent: Rethinking Verifiable Parental Consent Under the DPDP, 2023” (*Law School Policy Review*, 4 December 2025) <https://lawschoolpolicyreview.com/2025/12/04/the-curious-case-of-common-consent-rethinking-verifiable-parental-consent-under-the-dpdp-2023/>.
- ²² “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” (2026) 9(3) IJLMH 4117 <https://ijlmh.com/paper/childrens-rights-in-the-digital-crosshairs-a-comparative-study-of-child-data-protection-under-indias-dpdp-act-2023-and-the-eus-gdpr-framework/> [author name to be added].
- ²³ “Local Privacy Laws in a Globalized World” arXiv:2605.27801 <https://arxiv.org/pdf/2605.27801> [authors to be added; preprint].
- ²⁴ Wouter Lueks, Stephan Dreyer, Hannes Federrath and Judith Simon, “Assessing Age Assurance Technologies: Effectiveness, Side-Effects, and Acceptance” (arXiv:2603.25695, 26 March 2026) <https://arxiv.org/pdf/2603.25695>.
- ²⁵ “Age verification and data protection: Far more difficult than it looks” (IAPP, 2026) <https://iapp.org/news/a/age-verification-and-data-protection-far-more-difficult-than-it-looks> [author and date to be added].
- ²⁶ Louis Kaplow, “Rules Versus Standards: An Economic Analysis” (1992) 42 Duke LJ 557.
- ²⁷ Daniel J Solove, “Introduction: Privacy Self-Management and the Consent Dilemma” (2013) 126 Harvard Law Review 1880.
- ²⁸ Ari Ezra Waldman, “Privacy Law’s False Promise” (2020) 97 Washington University Law Review 773.
- ²⁹ DPDP Act 2023, s 2; DPDP Rules 2025, r 2.
- ³⁰ DPDP Rules 2025, r 10.
- ³¹ NovoJuris, “Child’s Personal Data and Privacy: Analysing the Draft DPDP Rules, 2025” (4 February 2025) <https://www.novojuris.com/thought-leadership/child-s-personal-data-and-privacy-analysing-the-draft-dpdp-rules-2025.html>. The critique concerned the draft Rules.
- ³² DPDP Rules 2025, r 10, illustrations.
- ³³ DPDP Rules 2025, r 12 and Fourth Schedule, Part B.
- ³⁴ MediaNama, “DPDP Rules: Platforms need parental consent to use children’s data” (10 January 2025) <https://www.medianama.com/2025/01/223-data-protection-rules-2025-children-data-india/>. This commentary concerned the draft Rules.
- ³⁵ DPDP Act 2023, Schedule (entry on additional obligations in relation to children under s 9).
- ³⁶ *Shreya Singhal v Union of India* (2015) 5 SCC 1.
- ³⁷ DPDP Act 2023, Schedule (entry on additional obligations in relation to children under s 9); see Part II.C above.
- ³⁸ Kaplow (1992) 42 Duke LJ 557, discussed in Part III.C.
- ³⁹ DPDP Act 2023, s 6(1) and the Schedule.
- ⁴⁰ DPDP Act 2023, s 8, in particular the security-safeguard and erasure duties.
- ⁴¹ DPDP Rules 2025, r 10.
- ⁴² DPDP Rules 2025, rr 8 and 10 and Fourth Schedule.
- ⁴³ DPDP Rules 2025, r 12 and Fourth Schedule, Part B.
- ⁴⁴ DPDP Act 2023, ss 27 and 28.
- ⁴⁵ Ari Ezra Waldman, “Privacy Law’s False Promise” (2020) 97 Washington University Law Review 773, discussed in Part III.C.
- ⁴⁶ Daniel J Solove, “Introduction: Privacy Self-Management and the Consent Dilemma” (2013) 126 Harvard Law Review 1880.
- ⁴⁷ UN Committee on the Rights of the Child, General Comment No 25 (2021) on children’s rights in relation to

the digital environment, CRC/C/GC/25.

⁴⁸ Regulation (EU) 2016/679, arts 6 and 8 and recital 38.

⁴⁹ DPDP Act 2023, ss 7 and 9(1).

⁵⁰ European Data Protection Board, Statement 1/2025 on Age Assurance (February 2025).

⁵¹ Information Commissioner's Office, *Age appropriate design: a code of practice for online services* (2020), issued under the Data Protection Act 2018, s 123, in particular standard 3 (age appropriate application), standard 5 (detrimental use of data), standard 8 (data minimisation) and standard 12 (profiling).

⁵² Information Commissioner's Office, monetary penalty notice against TikTok (April 2023), £12.7 million. The penalty was challenged on appeal by the company.

⁵³ Regulation (EU) 2022/2065 (Digital Services Act) [2022] OJ L277/1, art 28.

⁵⁴ European Commission, Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(1) of Regulation (EU) 2022/2065 (14 July 2025) <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>.

⁵⁵ DSA Observatory, "The Commission's approach to age assurance: Do the DSA Guidelines on protecting minors online strike the right balance?" (31 July 2025) <https://dsa-observatory.eu/2025/07/31/do-the-dsa-guidelines-on-protecting-minors-online-strike-the-right-balance/> [author name to be added].

⁵⁶ Children's Online Privacy Protection Act, 15 USC 6501–6506; 16 CFR Part 312, in particular ss 312.2 (definitions, including "directed to children" and actual knowledge), 312.5(b) (methods of verifiable parental consent), 312.11 (safe harbour programmes) and 312.12 (approval of new methods). The FTC's 2025 amendments to the Rule carry a compliance date of April 2026.

⁵⁷ *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1; *Justice K S Puttaswamy (Retd) v Union of India* (2019) 1 SCC 1 (Aadhaar).

⁵⁸ Chambers and Partners, "MeitY plans to cut short DPDP Compliance Timeline and Notify Cross Border Restrictions for SDFs" (22 February 2026) <https://chambers.com/articles/meity-plans-to-cut-short-dpdp-compliance-timeline-and-notify-cross-border-restrictions-for-sdfs>; DPDP Rules tracker <https://dpdpa.dcomply.in/rules/> (site reporting verification on 8 September 2026 and that the proposal had not been notified). These are secondary sources, and the position may change.

⁵⁹ DPDP Act 2023, ss 32 and 33(2).

WHITE BLACK
LEGAL