



The Dialogue®  
INFORM ENGAGE IDEATE

EVENT REPORT

# CONFERENCE ON CHILDREN'S PERSONAL DATA PROTECTION

February, 2025



EVENT REPORT

# CONFERENCE ON CHILDREN'S PERSONAL DATA PROTECTION

(C) 2025 THE DIALOGUE. ALL RIGHTS RESERVED.

**The Dialogue** is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

**For more information**

Visit [thedialogue.co](http://thedialogue.co)

**Suggested Citation**

*Event Report: Conference on Children's Personal Data Protection* (February, 2025). The Dialogue.

**Catalogue No**

TD/PDG/ER/0225/03

**Publication Date**

February 24, 2025

**Disclaimer**

The facts and information in this report may be reproduced only after giving due attribution to The Dialogue.

# CONTENTS

<i>1. Introduction.....</i>	<i>1</i>
<i>2. Panel 1: Impact of Verifiable Parental Consent Provisions on Start-ups and MSMEs.....</i>	<i>2</i>
<i>3. Panel 2: Enhancing Children's Personal Data Protection - An Optimal Way Forward.....</i>	<i>3</i>
<i>4. Key Takeaways and Future Directions.....</i>	<i>4</i>

# 1. INTRODUCTION

The Conference on Children's Personal Data Protection, organised by the Dialogue on February 18, 2024, gathered experts from various sectors to explore the challenges and solutions related to Rule 10 of the DPDP Rules, which focuses on obtaining parental consent for collecting children's personal data. Key discussions revolved around the practicality of parental consent mechanisms, age verification standards, the adoption of risk-based approaches, and the delicate balance between privacy and online safety for children. The event featured two-panel discussions and a keynote address that highlighted the broader objectives of the regulation while stressing the importance of developing practical and effective solutions. We were delighted to host the following individuals as speakers at this conference:

**Keynote Address:** Mr. Vikash Chourasia, Scientist D, MeitY

## Panellists

1. Mr. Subhodeep Jash, Associate Vice President (AVP) of Policy and Alliances, Convegenius
2. Ms. Uthara Ganesh, Head of Public Policy, Snap
3. Mr. Rakesh Maheshwari, Former Cyber Laws Coordinator, MeitY
4. Ms. Tamoghna Goswami, Director - Policy, ShareChat
5. Ms. Aparajita Bharti, Co-founder, The Quantum Hub
6. Mr. Hoonar Janu, Head of Policy, Info Edge
7. Mr. Shatakratu Sahu, Senior Research Analyst/ Senior Program Manager, Carnegie India

## 2. PANEL 1: IMPACT OF VERIFIABLE PARENTAL CONSENT PROVISIONS ON START-UPS AND MSMEs

Through this panel, we discussed the impact of Rule 10 on emerging and smaller players in the ecosystem. The panellist pointed out that Rule 10(1)(a) default does not apply to small players, including start-ups and MSMEs, as they may not pose extensive user data. This leaves smaller players with virtual tokens as the only means to obtain Verifiable Parental Consent (VPC), with less room for alternatives. They mentioned how this could create product friction, leading to user drop-off during sign-ups. For instance, a panellist highlighted that a lack of alternatives might lead to a situation where data fiduciaries may face dropouts as the number of clicks to enrol may increase with the virtual token mechanism.

The panellists pointed out that Rule 10(1)(b), which mandates the use of government-issued IDs for verification, could promote data maximisation, heighten privacy risks and pose scalability concerns. They proposed alternatives like a tiered verification system based on platform risk levels, including stricter checks for high-risk platforms like gambling sites and more lenient methods for lower-risk ones like educational tools. Additionally, they discussed challenges for platforms like social media apps that lack parental data and must rely on third-party verification systems.

Another key issue was defining a “child” in the digital world. Some argued that 16 and 17-year-olds should be treated differently from younger

children, suggesting more nuanced consent mechanisms. The panel also raised concerns about parental digital literacy, especially in tier 2,3 and 4 cities, which could lead to unintended exclusion from online services.

The discussion explored whether collaboration between the government and platforms could enable verifiable consent without collecting excessive data. Some suggested using device—or app-store-level verification methods, although questions arose about their practicality in India, where shared devices are common.

A larger concern was that parental consent alone is insufficient to ensure children's online safety. The panellists advocated for design-based solutions like privacy-focused advertising models and frameworks for age-appropriate content to foster a digital environment for kids.

Therefore, the panel agreed that to fix the status quo, it is important to expand the options through which data fiduciaries can verify the parent of the child. Exploring alternative options under Rule 10 would allow data fiduciaries to adopt less intrusive, scalable, and user-friendly mechanisms without causing friction depending on the nature of the service.

### 3. PANEL 2: ENHANCING CHILDREN'S PERSONAL DATA PROTECTION - AN OPTIMAL WAY FORWARD

The second panel explored solutions and strategies for effectively implementing Rule 10. A major concern was the cost and scalability of stringent age verification systems, especially for smaller platforms and MSMEs. The panel highlighted approaching VPC mechanisms from a top-down lens, i.e., developing options for VPC keeping larger data fiduciaries in mind would cause friction to smaller data fiduciaries due to practical incompatibility in applicability. For instance, a panellist mentioned that being an MSME makes it difficult for them to obtain VPC using virtual tokens, which may lead to dropouts. Therefore, the panel emphasised that policy must not be made with large companies in focus but should account for smaller firms such that it does not entrench larger players and support smaller players.

To address this, a principle-based approach was proposed, allowing flexibility based on platform type and risk level, helping to reduce implementation friction. They also discussed the complexity of balancing child safety, privacy, and platform usability. They raised concerns about Aadhaar-based verification and potential privacy issues when combined with APAAR IDs (which store academic records), leading to data maximisation risks.

The panel also examined global practices, highlighting diverse approaches to parental consent verification. The discussion highlighted various opinions on the preferred method to verify parental consent within the EU itself. For instance, an EU-based survey revealed that facial recognition was the best method, whilst credit card information was the worst. However, a France-based study, on the other hand, revealed that no particular method could be described as the best. These experiences confirm how the correct practice of acquiring parental consent is still an

ongoing exercise and brings various kinds of concerns to the floor. A graded approach to age verification was suggested, where different verification levels would apply based on the risk profile of the platform.

While self-regulation could offer flexibility, the panellist suggested the need for government oversight with opportunities for industry participation to balance compliance and practicality.

The panel highlighted the importance of leveraging India's Digital Public Infrastructure (DPI) to develop seamless, privacy-preserving verification systems. One proposed solution was tokenised parental consent, allowing platforms to verify parental approval without storing excessive personal data, thus maintaining privacy. However, the panel also discussed that leveraging DPIs for delivering VPC might cause exclusion for various reasons, including lack of scalability, technical capacity, and accessibility.

To ensure the effectiveness of any proposed solutions, panellists advocated for a pilot or sandbox approach before full-scale implementation. This would allow stakeholders to test systems, gather feedback, and refine policies based on real-world scenarios, ultimately leading to more effective and contextually appropriate strategies for Rule 10.

Besides, it was also suggested that provisions within Rule 10 be further diluted and that the government consider introducing a more comprehensive framework to protect child safety, security, and privacy, similar to the Age-appropriate design code of the United Kingdom, which would comprehensively set the standards for online services.

## 4. KEY TAKEAWAYS AND FUTURE DIRECTIONS

- 1. Impact on Smaller Data Fiduciaries:** Smaller data fiduciaries are disadvantaged when securing verifiable parental consent for processing children's data and verifying parents' identities.
- 2. Expand Rule 10, allowing diverse Parent Verification Methods:** A universal solution may not be practical. Instead, adopting a risk-based, tiered approach to age verification is recommended. Also, the mechanism must start from the least common factors to scale up. For instance, allowing data fiduciaries to register a new account for parents while verifying their age and identification.
- 3. Building an Age-Appropriate Design Standard for India:** While parental consent is a starting point, it isn't enough. The ecosystem should incorporate age-appropriate design standards to protect children online. Therefore, panellists discussed the need to develop a comprehensive age-appropriate design code for India.
- 4. Exploring Alternatives to ID-Based Verification:** Relying solely on Rule 10(1)(b) could lead to excessive data collection and lead to exclusion. Options like tokenised consent or device-level verification offer more privacy-conscious alternatives. Alternatively, options like cross-sign-up methods where small platforms can use the reliable information held by larger platforms for VPC were suggested.
- 5. Collaboration Between Government and Industry:** Effective age verification requires joint efforts between regulators and platforms to create practical, scalable solutions.
- 6. Phased Implementation Strategy:** Using a sandbox model or pilot programs can help test and refine Rule 10 before rolling it out on a larger scale.

The conference highlighted the need to balance regulatory goals with practical execution. As India's DPDP framework continues evolving, stakeholders must collaborate to develop effective, privacy-preserving, and scalable solutions to safeguard children's online experiences.

# ENHANCING PARENT VERIFICATION AND CHILD DATA PROTECTION

## Policy Considerations and Implementation Strategies



### IMPACT ON SMALLER DATA FIDUCIARIES

Smaller data fiduciaries may face difficulties in securing verifiable parental consent for processing children's data and challenges in verifying parents' identities.



### EXPAND RULE 10: ALLOWING DIVERSE PARENT VERIFICATION METHODS

A universal solution may not be practical. Adopt a risk-based, tiered approach to age verification. Start with least common factors and scale up. Example: Allow data fiduciaries to register a new account for parents while verifying their age and identity.



### BUILDING AN AGE-APPROPRIATE DESIGN STANDARD FOR INDIA

Parental consent alone is not enough to protect children online. The ecosystem needs a comprehensive age-appropriate design code.



### EXPLORING ALTERNATIVES TO ID-BASED VERIFICATION

Sole reliance on Rule 10(1)(b) can lead to excessive data collection and exclusion. Privacy-conscious alternatives include tokenised consent, device-level verification, and cross-sign-up methods, where smaller platforms use reliable data from larger platforms for verification must be considered.



### COLLABORATION BETWEEN GOVERNMENT AND INDUSTRY

Effective age verification needs joint efforts between regulators and platforms. Solutions must be practical and scalable.



### PHASED IMPLEMENTATION STRATEGY

Implement sandbox models or pilot programs to test and refine Rule 10 before full rollout.



[thedialogue.co](http://thedialogue.co)



[LinkedIn | The Dialogue](#)



[X | The Dialogue](#)



[Whatsapp | The Dialogue](#)



[Instagram | The Dialogue](#)