REGIONAL CONSULTATION ON

VERIFIABLE PARENTAL CONSENT

WHITE PAPER

JAN 2025

SPACE2GROW
Consulting for Good

PACTA
SOCIAL | IMPACT | LEGAL

01. INTRODUCTION

The Digital Personal Data Protection (DPDP) Act 2023, notified in the official gazette, marks a significant step in safeguarding personal data. The DPDP Act provides a legal framework to protect the digital personal data of individuals in India. Under Section 9(1) of the DPDP Act, parental consent is mandated before processing the personal data of a child, defined as anyone under the age of 18.

> *"Section 9 (1) - The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed."*

The consultations were conducted in November and December 2024 to bring in the voices of parents and their thoughts and challenges in providing consent and verifiable consent. The platforms face the challenge of balancing legal compliance with the practical complexities of verifying parental consent in India's diverse digital landscape, and the need for accessible and easy solutions is critical.

The consent of the parent includes the consent of the lawful guardian, wherever applicable. While the act has established the need for parental consent, the Ministry of Electronics and Information Technology (MeitY) has now specified the same in the draft Rules released. The consultation and the outcomes align with draft Rules, and now it's important to collaborate and see how platforms design effective solutions

Challenges to Effective Consent Verification in India

01	**Impact on Rural Areas:** Low digital literacy among rural parents and shared device usage with a 78% increase in shared device usage in rural India in 2023 mean children often navigate digital spaces on behalf of their parents. A recent study by Space2Grow revealed a high proportion of parents and teachers, specially in the rural areas being unaware of digital safety. This increases the likelihood of bypassing age restrictions, undermining the intent to protect minors.
02	**Gender Barriers**: According to ASER 2023 report, boys in rural areas are twice as likely to own smartphones compared to girls. Complex consent processes may discourage parents from including girls in online activities, further widening the gender gap in access to education and digital opportunities. However, a study by Space2Grow revealed gender neutrality to internet access with overall 99% children aged 13-17 having access. This shows that even if girls are not owning devices they have access to the internet through shared devices.

03	**Lack of Standardisation:** With platforms designing their own consent mechanisms, parents may face varied and often confusing processes. This lack of uniformity increases frustration, particularly for less tech-savvy users.
04	**Challenges for Vulnerable Children:** For children without direct parental oversight, such as those in foster care or institutional homes, verifying parental consent is difficult. Unclear guardianship structures may exclude them from digital platforms altogether.
05	**Safeguarding Children's Autonomy:** While parental consent is crucial for protecting children's data online, overly complex methods could unintentionally hinder their autonomy. Children, especially teenagers, often navigate educational and social platforms for learning and personal growth. If parental consent mechanisms are cumbersome or overly restrictive, it may limit their ability to freely explore these spaces.

Given India's diverse socio-economic landscape and recognising the need for practical solutions, Space2Grow and PACTA engaged with key stakeholders- parents, NGOs, and community organisations, to gain a deeper understanding of grassroots realities. The consultations focused on exploring effective approaches for obtaining parental consent on digital platforms while addressing the practical realities of shared device usage, low digital literacy, and gender divides. The overarching aim was to identify possible solutions that can work across different socio-economic groups, especially marginalised ones, to ensure that effective and inclusive methods are identified.

02. METHODOLOGY

To gain an understanding of verifiable parental consent, a series of regional consultations were conducted, with stakeholders from diverse backgrounds and capturing perspectives from different socio-economic and regional contexts.

Stakeholders involved

Parents and legal guardians of children aged 13-17 years across India participated in the consultation. One consultation was conducted in each region–North, South, East, West, and Northeast, with 20 participants per session, totalling **100 participants**. A deliberate effort was made to include a balanced mix of rural, urban, and lower-income group parents to capture diverse socio-economic perspectives and to gain the perspective on varied realities faced by families across regions.

One nationwide consultation was conducted with **15 NGOs** working in Child Protection, Digital Safety and related fields.

Session details

During the consultation, a session was delivered on the importance of personal data, and digital consent, and the Digital Personal Data Protection Act (DPDP Act) 2023 with a focus on Section 9 (1) of the Act. The session focused on two components of verifiable parental consent, consent collection and verifying parental identity. The session was followed by a Focus Group Discussion (FGD) to understand what methods would be feasible for consent collection and verifying parents' identity.

The methods recommended to obtain verifiable parental consent by the Federal Trade Commission under the Children's Online Privacy Protection Act (COPPA) were shared during the session with NGOs as well as parents. Additionally, the recommended methods of seeking verifiable parental consent from the findings of The Quantum Hub (TQH) and Young Leaders for Active Citizenship (YLAC) report "Navigating Children's Privacy and Parental Consent under the DPDP Act 2023" and Youth Ki Awaaz report "Balancing Consent and Customisation" were also shared with the participants.

Suggestive methods of consent collection

Some of the methods of consent collection shared with the participants include:

01 Consent Form (Digital)	02 Consent Form (Print and Send)	03 Toll-free Number
A consent form to be digitally signed by the parent.	A consent form to be printed, signed by the parent which can be sent back via, mail, or electronic scan.	Parents will call a toll-free telephone number staffed by trained personnel to give the consent.

04 Preferences and filters through a third-party service	05 Video Conference
Parents define their children's preferences and filters through a third-party service, which works with the platforms to provide consent and curate the content that will be shown to the children.	Parents will connect to trained personnel via video-conference and give their consent

Suggestive methods of verifying parental identity

Some suggestive methods of verifying parental identity while giving consent were shared with the parents to identify their preferred methods.

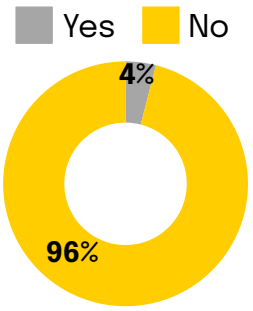
01 Verification by Govt ID against the existing database	02 Verification by Govt ID Card followed by facial recognition	03 One -Time Verification by Govt ID Card on Play Store/App Store
Verifying a parent's identity by checking a government-issued ID like aadhar card, pan card, etc, against databases of such information.	Verifying a picture of a government photo ID submitted by the parent and then comparing that photo to a second photo submitted by the parent, using facial recognition technology.	Parents will have to upload their Government ID card on the Play Store/App Store. The Play Store/App Store will verify the age and take the consent. This may not include the web applications.

04 Self-declaration by the child followed by OTP	05 Govt ID (Aadhaar) and OTP-based Verification
The child user can give a self declaration and can input the parent's mobile number or email ID. The parents will need to share the OTP received on their mobile number or email ID.	Parents will have to add their name and last four digit of the aadhar card. An OTP will be received on the mobile number linked to the Aadhaar card.

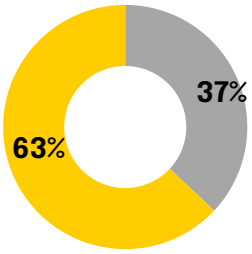
03. KEY FINDINGS

Awareness and Perception of Data Privacy

The digital age has created a paradox where access is easy, but understanding is scarce–only 4% of respondents believe it is safe to share personal data without reading the Terms and Conditions, while an overwhelming 96% think it is unsafe. This reflects a growing awareness among parents about the risks of blindly agreeing to digital contracts. However, when it comes to children, 63% of respondents believe they do not read Terms and Conditions.



Is it Safe to share data without Reading Terms and Conditions?



Do children read the Terms and Conditions

During consultations, parents expressed concerns about children's impulsiveness online. One parent shared, "*These documents are so long and technical, even I struggle to read them. How can we expect children to?*" These insights underline the critical role of verifiable parental consent in ensuring that platforms are accountable for safeguarding children's data. Such consent should be informed, time-bound, and hassle-free, enabling parents to make clear, well-understood decisions without unnecessary complications, particularly in contexts where children may unknowingly bypass protections.

Protecting Children's Sensitive Data: Parental Concerns and Compliance

When asked about the types of digital personal data they are most concerned about regarding their child's safety online, the top three concerns were **passwords**, **photos and videos**, and **location**. These concerns reflect a heightened awareness among parents about the risks of security breaches, tracking, and exploitation, which can result from mishandling of such sensitive data. The DPDP Act ensures that parents are informed and empowered to make decisions about their child's data.

Parental Preferences for Consent Collection Methods

The consultation explored parental preferences for various methods of providing consent. The top two preferred methods identified by respondents were:

Consent Form: Consent forms, whether submitted digitally or in printed format, emerged as the most preferred method for obtaining parental consent. This process involves parents receiving a consent form, filling it out, and returning it either online or through physical means. This method accommodates both tech-savvy parents and those in rural or low-literacy areas, as parents are already accustomed to form-based processes for schools, government services, and other formal systems. However, handling offline consent forms–can be resource-intensive for platforms managing a large number of users, requiring robust systems for tracking and verification.

Video-Conference: Video conferencing emerged as the second most popular method for obtaining verifiable parental consent. This approach involves parents engaging in a live video interaction with platform representatives to provide consent. Parents value direct, face-to-face engagement as it allows them to verify the legitimacy of the process, and build trust with the platform. For platforms, scaling this method for large user bases can be resource-intensive.

Preferred with Parental Verification Processes

When it comes to verifying parental consent, parents displayed a range of preferences driven by trust, security, and familiarity with existing systems. **Aadhaar and OTP-Based Verification** stood out as the most favored method, chosen by 36% of respondents, due to its simplicity and the widespread trust in government-backed systems.

However, parents' comfort levels in sharing their government IDs for verification purposes revealed important nuances. 57% of parents expressed some level of comfort (26% very comfortable, 31% somewhat comfortable) sharing their government-issued IDs for verification purposes. But, 25% remained neutral, and 18% felt uncomfortable (15% somewhat uncomfortable, 3% very uncomfortable), citing privacy concerns and the potential for misuse of sensitive information.

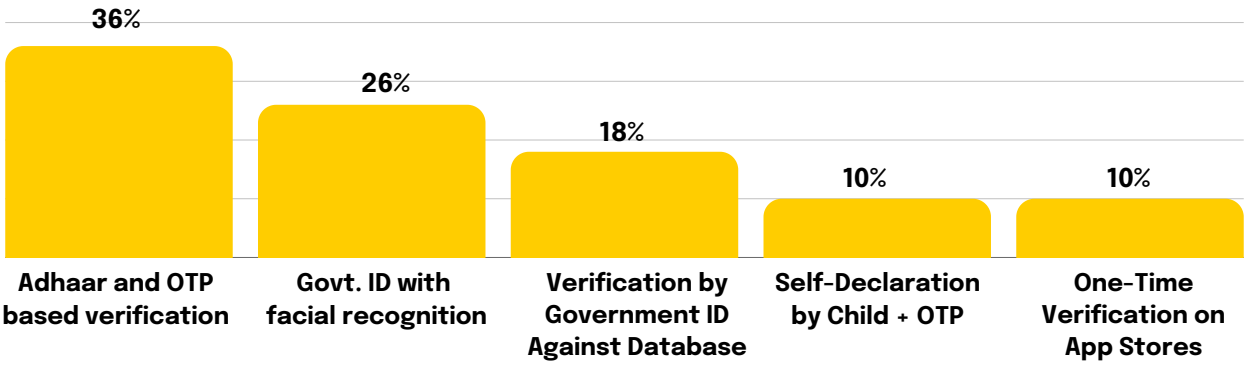
One parent highlighted their concern, stating, “Aadhaar is something we rely on for essential services like banking, so I am not very comfortable sharing it with random platforms”. Another parent coming from an Army background also shared that due to security reasons they are not very comfortable sharing their government-issued IDs with unknown platforms. A suggestion that came up was that listing out safe platforms by the government would help build trust among parents to share their IDs for verification and not worry about misuse for platforms that are marked safe by the government.

The second most preferred method was **Verification by Government ID with Facial Recognition**, supported by 26% of respondents. Parents appreciated the enhanced security of biometric verification in preventing the bypass of verification systems by children. However, concerns about data privacy were voiced, with 44% of parents were comfortable sharing their biometric data (26% very comfortable, 18% somewhat comfortable), concerns about privacy and security were more pronounced, with 31% feeling uncomfortable (15% somewhat uncomfortable, 16% very uncomfortable) and 25% remaining neutral.

The third choice, **Verification by Government ID Against a Database** (e.g., DigiLocker), was favoured by 18% of respondents. While some parents recognised the credibility of government platforms like DigiLocker, others found them unfamiliar, especially in rural areas.

The least preferred were **Self-Declaration by Child** and **One-Time Verification on App Stores**, each supported by only 10% of respondents. Parents viewed these methods as inadequate, with one parent remarking, "*Children can easily bypass these systems, then what's the point for designing privacy measures*"

These responses highlight the need for verification systems that balance security, accessibility, and privacy concerns.



04. RECOMMENDATIONS

Suggested Framework for Verifiable Parental Consent

To align with the DPDP Act, 2023, specifically Section 9(1) mandating verifiable parental consent, a comprehensive and inclusive framework is essential. The following stepwise framework leverages Aadhaar and OTP-based verification to ensure trustworthiness, simplicity, and scalability while addressing India's socio-economic and digital diversity.

Step 1: Initiating the Consent Process

- Trigger for Consent: Platforms prompt for consent whenever a child signs up for a platform or service that collects, processes, or stores personal data.
- Consent Form: Parents/Guardians fill out a basic digital consent form, specifying their details, including name, last four digits of the Aadhaar number, and contact information (mobile number linked to Aadhaar).

Step 2: Aadhaar-Based Identity Verification

- OTP Generation: An OTP (One-Time Password) is generated and sent to the parent/guardian's Aadhaar-linked mobile number.
- OTP Submission: Parents/Guardians enter the OTP on the platform to confirm their identity. The system cross-verifies the OTP with Aadhaar's secure backend infrastructure to ensure authenticity.

Step 3: Consent Confirmation

- Consent Agreement: Parents/Guardians are shown a clear summary of how the child's data will be collected, processed, stored, and used. This is presented in simple language and multiple regional languages to ensure accessibility. Parents confirm their consent by digitally signing or selecting an "I Agree" option.
- Record Generation: A secure digital record of the parental consent is generated and stored by the platform for compliance purposes.

Step 4: Data Minimisation and Safeguards

- Data Collection Transparency: The platform collects only the necessary information required for the service, in alignment with the DPDP Act's principles of data minimisation and purpose limitation.
- Parental Dashboard: Platforms provide parents with a dashboard to review, manage, and revoke their consent if needed.

Step 5: Renewability

- Time-Bound Consent: Parental consent is valid for a predefined period (e.g., one year). Parents are notified before the expiry to renew consent or withdraw it.

Step 6: Support Mechanisms for Inclusivity

- Multilingual Support: Platforms ensure the consent process is available in multiple languages to cater to India's linguistic diversity.
- Helpdesk and Helpline: A toll-free helpline or chat-based support can guide parents through the process and address concerns about data privacy and security.

Limitations of this Framework

01	This approach assume that children will honestly declare their real age. However, there is high chance that children may try to game the system.
02	One significant limitation of the framework lies in its underlying assumption that parents are actively involved in managing their children's digital data and providing consent. This assumption may not hold true for low-resource households where parents often lack digital literacy or access to the necessary infrastructure. Furthermore, this model may exclude children in institutional care, foster homes, or other vulnerable settings where clear parental oversight is either absent or inconsistent. Risks of parents using the withdrawal of consent as leverage to influence children's actions.

What Platforms can Do?

- **Transparency in Data Collection**: Platforms must clearly inform parents about why data such as passwords, photos, videos, and location is being collected, how it will be used, and the duration for which it will be stored. Such transparency builds trust and aligns with the DPDP requirement for clarity and accountability in data handling.

- **Purpose Limitation**: Platforms should strictly adhere to the principle of data minimisation, collecting only the data that is necessary for the intended purpose.

- **Secure Storage and Processing**: Platforms must implement robust data security measures to protect sensitive data from breaches. This includes encryption of passwords, secure servers, and anonymising location data when possible. These practices align with the DPDP's emphasis on safeguarding personal data

- **Disallowing Targeted Advertisements**: Platforms must disallow targeted advertisements or content aimed at children. This ensures that children are not subjected to manipulative marketing practices and helps create a safer, more ethical digital environment that prioritises their well-being over commercial interests.

- **Separation of Consent for Data Sharing and Service Access**: Platforms must ensure that verifiable parental consent for processing children's data is not conflated with consent for accessing digital services. Mechanisms should evolve to clearly separate these two forms of consent, ensuring that parents or guardians can make informed decisions about data sharing without restricting children's access to essential digital services.

- **Parental Control**: Platforms that have a user base amongst minors should offer parents tools to manage their child's data, such as dashboards to view what data is collected and easily accessible options to revoke consent or delete data when necessary.

- **Regular Audits and Compliance Checks**: To comply with DPDP guidelines, platforms must conduct regular audits of their data processing practices to ensure they remain compliant and secure.

05. CONCLUSION

The Digital Personal Data Protection Act, 2023 (DPDP Act), marks a significant leap toward protecting the personal data of individuals, including children, in India's rapidly evolving digital ecosystem. Central to this is the mandate for verifiable parental consent, a measure aimed at ensuring that the data of minors is handled responsibly. This white paper explores the complexities and realities of implementing verifiable parental consent, drawing from extensive consultations with parents, NGOs, and community organisations across India. The findings highlight critical challenges while providing actionable recommendations for seeking verifiable parental consent.

The findings outlined in this white paper highlight the need for **standardisation in the consent mechanism**. Building localised systems with simple, user-friendly interfaces in regional languages will help make consent processes accessible to all. By mandating standardised verification processes across platforms, confusion can be minimised, and trust strengthened among parents managing multiple systems. Given the low levels of knowledge amongst parents regarding digital personal data and digital consent, community-led, multi-channel awareness campaigns are critical to educating parents and caregivers about the importance of parental consent and guiding them through these systems step-by-step.

The consultations revealed that parents prefer **Aadhaar and OTP-based verification emerged as the most favoured approach** due to its simplicity and reliance on government-backed systems. However, this method has certain limitations such as this system assumes that children will declare their actual age honestly and some parents shared their apprehensions about sharing their Aadhaar details with different platforms.

The recommendations for tech platforms presented in this paper align closely with the DPDP rules, which emphasise transparency, data minimisation, and inclusivity. The Act's insistence on clear, simple language in data processing agreements resonates with the need for user-friendly consent mechanisms. Similarly, its focus on safeguarding data through robust technical and organisational measures underscores the importance of integrating techno-legal frameworks into consent systems.

However, it is important to recognise that achieving compliance with the DPDP Act does not eliminate the broader risks children face online. Cyberbullying, exploitation, and exposure to harmful content remain persistent threats that require sustained vigilance. Furthermore, the socio-cultural nuances of India's digital divide–such as the gender gap in smartphone access and varying levels of digital literacy–demand targeted interventions. Efforts to implement verifiable parental consent must address these intersectional factors to avoid unintentionally excluding marginalised communities from the benefits of digital safety initiatives.

SPACE 2 GROW
Consulting for Good

PACTA
SOCIAL | IMPACT | LEGAL