Verifiable consent for processing personal data of children under the DPDP Act

The regulation of children's access to social media platforms is rapidly becoming one of the most closely watched areas of digital policy. Governments across jurisdictions are increasingly concerned about the impact of unrestricted social media access on children, including risks relating to privacy, harmful or age-inappropriate content, online addiction, cyberbullying, and manipulation through targeted algorithms.[1]

As a result, regulators are moving away from the earlier model where the platforms, based on certain criteria, would prescribe a minimum age threshold and rely upon the users to truthfully and correctly self-declare their age to access the matter.

Different jurisdictions, however, are taking different approaches to achieve this objective. Some have adopted prohibition-led models, while others have preferred consent-led frameworks.[2] Irrespective of the approach, the common denominator seems to be that businesses are expected to do more than simply treating age-gating as a formality.

VARIED APPROACHES: OUTRIGHT RESTRICTIONS v. PARENTAL CONTROL MODELS

At one end of the spectrum are jurisdictions such as Australia, which have moved towards stricter age-based restrictions for minors to access certain platforms.[3] Recent reforms seek to prevent younger users from holding accounts on certain social media services, placing the clear onus on platforms to implement reasonable measures to stop underage users from accessing such services. This model reflects a policy choice that some digital environments may pose sufficiently high risks to minors that parental consent alone may be inadequate. Instead, the burden is shifted to platforms to build systems that meaningfully prevent underage participation.

[1] *"Too young to scroll? Why governments are cracking down on social media age limits",* OECD, available at https://www.oecd.org/en/blogs/2025/06/too-young-to-scroll-why-governments-are-cracking-down-on-social-media-age-limits.html
[2] *"Social media age restrictions for children: Why they are rising and what comes next"*, OECD, available at https://www.oecd.org/en/blogs/2026/04/social-media-age-restrictions-for-children-why-they-are-rising-and-what-comes-next.html
[3] Online Safety Amendment (Social Media Minimum Age) Act, 2024, available at https://www.legislation.gov.au/C2024A00127/asmade/text

Other jurisdictions have preferred a parental control model. Under this approach, minors are not categorically excluded from accessing digital services, but their access is conditioned on parental or guardian consent, usually backed by some form of verifiable consent mechanism. The rationale here is that parents or guardians are better placed to decide whether a child should use a particular platform and on what terms. India's Digital Personal Data Protection Act, 2023 (**DPDP Act**) broadly falls within this second category.

INDIA'S POSITION UNDER THE DPDP ACT

With the aim of safeguarding interests of the children, the DPDP Act introduces child-specific compliance requirements that have significant implications for social media platforms, gaming companies, ed-tech providers, streaming services, and other online businesses which involve substantial access and participation by the younger population.[4]

Under the DPDP Act, a "child" means an individual who has not completed eighteen (18) years of age.[5] This age threshold is higher than in some other jurisdictions where the prescribed age is often under thirteen (13)[6] years or sixteen (16) years.[7] As a result, a large category of teenage users, who may otherwise be treated as independent users elsewhere, fall within the child-protection framework in India so far as the DPDP Act is concerned.

Under the DPDP Act, a data fiduciary must obtain 'verifiable consent'[8] of the parent or lawful guardian before processing the personal data of a child. This means that where a platform processes personal data in order to create accounts, enable interactions, personalize content, serve advertisements, track activity, or otherwise provide services; it will first need to ensure valid verifiable consent by parents/guardians is obtained if the user is under eighteen years of age.

This raises an important operational question: how does a business know whether the user is in fact under eighteen, and how does it reliably confirm that the consenting adult is genuinely the parent or lawful guardian?

WHY SIMPLE SELF-DECLARATION MAY NOT BE ENOUGH UNDER THE DPDP ACT?

Historically, many platforms have used a basic age-screening model. Users are asked to declare their date of birth during sign-up or accessing the content. If the declared age is above the threshold, the access is allowed and the platform processes the personal data based on such declaration.

Although the DPDP Act does not prohibit businesses from implementing self-declaration models; in practice, this model presents a likely risk of circumvention if the information provided at the time of self-declaration is false. Relying solely on self-declared information, despite obvious risks of circumvention, comes with a possibility of regulatory scrutiny to assess adequacy and effectiveness of child-protection measures. Therefore, it is critical for businesses to carefully assess and adopt suitable measures to meaningfully comply with their legal obligations while processing children's personal data.

[4] For a detailed discussion on child-specific obligations under the DPDP Act, please refer to our previous primer, available at https://elplaw.in/wp-content/uploads/2025/12/Processing-of-childrens-personal-data-under-the-DPDP-Act-what-does-it-means-for-businesses.pdf
[5] Section 2(f), DPDP Act.
[6] For example, in the USA, The Children's Online Privacy Protection Act (**COPPA**), defines an individual under the age of thirteen (13).
[7] For example, in the European Union (**EU**), General Data Protection Regulation (**GDPR**) defines a child as an individual below the age of sixteen (16) years, with flexibility for EU Member States to lower this threshold to thirteen (13) years.
[8] Section 9, DPDP Act.

VERIFYING PARENT'S OR GUARDIAN'S IDENTITY UNDER THE DPDP ACT?

While the businesses are expected to implement *'appropriate technical and organizational measures'* to ensure that the verifiable consent being provided on behalf of a child is that of parents or the lawful guardian. As per the Digital Personal Data Protection Rules, 2025, (**DPDP Rules**), the veracity of the verification provided by parent or lawful guardian on behalf of the concerned child, may be established by relying on (i) information being provided by the individual themselves, (ii) details already available with the business (in case, the individual acting as a parent or lawful guardian is an existing user of the platform), or (iii) virtual tokens of such details issued by authorized entity.[9]

Scheme of verifiable consent under the DPDP Act and DPDP Rules

Verify age of a user.

↓

If the user is a child, seek verifiable consent of the parent or lawful guardian.

↓

Verify if the individual posing as parent or lawful guardian on behalf of a child is credible.

↓ ↓

If the parent or lawful guardian is already a registered user of the business, then the business can verify using those details.

If the parent or lawful guardian is not a registered user of the business, then such parent or lawful guardian can provide virtual tokens mapped to their identity and age through services like Digital Locker to the business for verification.

A flowchart capturing the step-by-step process of obtaining a verifiable consent

WHAT SHOULD BUSINESSES DO IN PRACTICE?

To effectively comply with the child-centric protection measures under the DPDP Act, the businesses will have to adopt a model keeping in mind the nature of the business and age of their primary users. Whether a business has significant or limited access to children's digital personal data, having a system to effectively obtain verifiable consent is a must to ensure compliance with the requirements of DPDP Act. Since the DPDP Act or DPDP Rules do not prescribe the mechanism for verifiable consent, the businesses can adopt suitable measures, so long the legal requirement is met. While doing so, the businesses across sectors need to be mindful about the following:

[9] Rule 10, DPDP Rules.

Reassess age-identification mechanisms. As step one, the businesses should evaluate age verification methods, since self-declared age alone may be considered inadequate. Depending on the nature of the platform, more robust age-assurance mechanisms may be warranted, such as:

- Document-based verification like Aadhar verification;
- Facial age estimation tools (subject to privacy safeguards); or
- Third-party trust or identity providers.

Build verifiable consent flows. Where users are identified as minors, businesses should implement verifiable consent mechanisms that can withstand potential legal scrutiny. This may involve:

- Collecting parent or guardian contact details;
- Authenticating the adult through OTP, KYC-lite or other validation tools;
- Providing clear notices to parents or lawful guardians; and
- In case of change in scope of processing, re-obtain verifiable consent.

Segment child and adult user experiences. Once child users are identified, platforms may need differentiated product journeys. This may include disabling targeted advertising; limiting profiling or tracking tools; providing enhanced reporting tools; and offering stronger privacy defaults.

Last but not the least, before adopting any specific consent management system (including verifiable consent mechanism), ensure that the system balances the requirements under the DPDP Act, while also maintaining the product quality, without compromising user experience.

We hope you have found this information useful. For any queries/clarifications please write to us at insights@elp-in.com or write to our authors:

Ravisekhar Nair, Partner – Email -ravisekharnair@elp-in.com

Abhay Joshi, Partner – Email - abhayjoshi@elp-in.com

Bhaavi Agrawal, Senior Associate- Email – bhaaviagrawal@elp-in.com