JUTA
POPIA PORTAL

ISSUE NO 75 • HOW OLD ARE YOU? THE PRIVACY PARADOX OF PROTECTING CHILDREN ONLINE • NOVEMBER 2026

HOW OLD ARE YOU? THE PRIVACY PARADOX OF PROTECTING CHILDREN ONLINE

1. INTRODUCTION

Children spend much of their lives online, where services routinely collect information about them. Protecting children may require an organisation to know whether a user is under 18, yet age checks can require additional personal information. This article considers that tension under POPIA, focusing on age assurance, minimality, privacy by design, and child-friendly transparency.



Photo: iStock

2. PROTECTING CHILDREN CAN REQUIRE MORE PERSONAL INFORMATION



Photo: iStock

Online age checks are rarely simple. A service may ask for a date of birth or identity document, use a third-party age-checking provider, or estimate age from a face or behaviour. These methods can support child-appropriate settings or restrict inappropriate content, but they also create privacy risks.

The question is not only whether age should be checked, but how to do so without collecting more personal information than necessary.

International regulators are paying close attention. In July 2025, the European Commission presented **guidelines for protecting minors online** and a prototype age-verification solution intended to let users prove they are over 18 without disclosing their exact age or identity.

The EDPB has also published age-assurance principles, including data minimisation, proportionality, and avoiding unnecessary identification.

Enforcement is increasing too. In August 2026, **Brazil's data protection authority fined ByteDance R$153.7 million** for infringements relating to TikTok's processing of children's and teenagers' data. For South African organisations, the practical question is: What conditions are required for the lawful processing of personal information when the data subject is a child?

3. POPIA GIVES CHILDREN ADDITIONAL PROTECTION


Photo: iStock

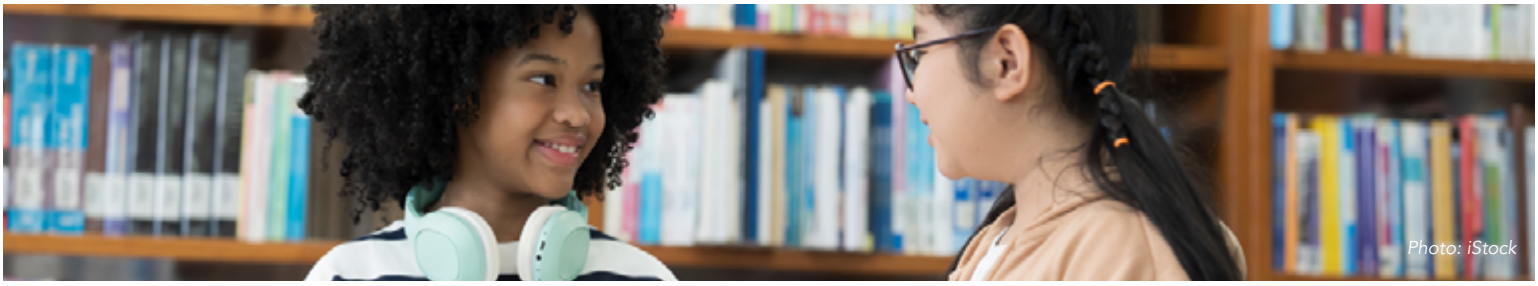
POPIA defines a child as a natural person under 18 who is not legally competent, without a competent person's assistance, to take any action or decision in respect of any matter concerning themself. A competent person is someone legally competent to consent to that action or decision, such as a parent or guardian.

Section 34 prohibits processing a child's personal information unless section 35 applies. Section 35(1) includes grounds such as prior consent from a competent person and processing necessary to establish, exercise or defend a right or obligation in law.

Consent from a competent person is important, but it is not the whole answer. The other conditions for lawful processing still apply, including POPIA's accountability requirement in section 8.

Section 35(3) also points to design. Where the Information Regulator authorises processing under section 35(2), it may require a responsible party to not encourage a child to disclose more personal information than is reasonably necessary and to maintain procedures to protect the information. Children's privacy should therefore shape the service, not only the legal basis.

4. AGE ASSURANCE MEETS MINIMALITY


Photo: iStock

4.1. What does the service actually need to know?

Section 10 of POPIA requires personal information to be adequate, relevant, and not excessive for the purpose. In age assurance, the first question is what the service actually needs to know.

If a service only needs to know whether a user is 18 or older, it should avoid collecting a name, identity number, exact date of birth, photograph or identity document unless those details are necessary for the risk being managed.

A system that confirms an age threshold without revealing identity can meet the purpose while processing less information. That is the logic behind the EU approach: the service receives proof of the relevant age attribute, not additional identity data.

4.2. What does compliant age assurance look like?

Age assurance includes self-declaration, AI or biometric systems, technical measures, third-party tokenised checks, and identifiers such as passports. Each method offers a different level of certainty and carries different privacy risks.

The method should match the risk. A low-risk service may not need the same assurance as a service exposing users to adult content or other significant harms. Self-declaration may be inadequate where underage access creates serious risk.

Organisations must also decide what happens after the check. If facial analysis is used, what happens to the image or information derived from it? What does a third-party provider retain? If an identity document is uploaded, is there a reason to keep it once the check is complete? The **UK ICO** recommends collecting only the minimum information needed and not using age-assurance information for unrelated purposes, which aligns with POPIA's minimality and purpose-specification requirements.

5. PRIVACY BY DESIGN REQUIRES MORE THAN AGE VERIFICATION



Photo: iStock

Age assurance matters only if the service changes when it knows, or has sufficient reason to believe, that the user is a child.

Depending on the service and risk, child-appropriate design may require more protective default settings, limits on geolocation, profiling and sharing, restrictions on contact from unknown adults, shorter retention periods, or changes to recommender systems. It may also require avoiding designs that encourage children to disclose information for rewards, game progress or social validation. Under POPIA, knowing that a user is a child should affect the processing that follows.

6. PRIVACY NOTICES: WHO IS THE AUDIENCE?



Photo: iStock

Photo: iStock

Once an organisation knows that it is processing a child's personal information, it should also ask for whom its privacy information is written.

Section 18 of POPIA requires a responsible party to take reasonably practicable steps to ensure that the data subject is aware of key information about the processing, including what is collected, why it is collected, relevant recipients, applicable rights, and the right to complain to the Information Regulator.

Privacy information is often directed to a parent or other competent person where consent is required. But the child remains the data subject. If the child uses the service and makes choices about their information, they should also receive information they can understand.

A privacy notice can meet section 18 and still fail in practice if it uses dense legal language, vague descriptions or information hidden behind several links.

The EDPB's March 2026 coordinated enforcement action on GDPR transparency and information obligations reflects the same point: transparency must be effective. For children, that means communication they can follow. A great example is LEGO's child-friendly privacy information page, which includes a video and a short, simple explanation of how LEGO uses personal information collected through cookies.

7. A CHILDREN'S PRIVACY-BY-DESIGN TEST



Photo: iStock

Organisations developing services that children may use can start with six questions:

- **Do we need to know the user's age?** Identify why age matters and what level of certainty the risk requires.
- **What is the least information we need?** Consider whether an age threshold can be established without collecting or retaining identity documents, exact dates of birth or unnecessary identifiers.
- **What changes because the user is a child?** Age assurance should trigger proportionate safeguards, including suitable defaults, limits on profiling and sharing, geolocation controls, retention limits, and recommender-system changes.
- **What happens to age-assurance information?** Limit retention and further use, assess providers carefully, and prevent age-assurance data from becoming profiling data.
- **Who needs to understand the processing?** Consider both the competent person and the child, because their information needs may differ.
- **Will they understand it?** Test the language, format, timing, and interface. Ask whether the processing would surprise the child or parent.

8. CONCLUSION



Photo: iStock

Protecting children online can justify stronger safeguards, including age assurance. But stronger protection should not become an excuse for disproportionate collection or surveillance. The aim is to establish age with enough confidence to manage the relevant risk while processing as little personal information as possible.

POPIA provides the building blocks for that approach. Its special rules for children sit alongside minimality, purpose specification, security safeguards, and openness. Read together, they ask a design question, not only a compliance question: how should the service work differently because the person using it is a child?

Consent from a competent person may make processing permissible, but it does not by itself make the service child appropriate. If a service is designed for children, its privacy should be designed for them too.

9. FURTHER READING



Photo: iStock

- **Chapter 6:** Processing must be for a lawful purpose
- **Chapter 7:** Special personal information and children's personal information
- **Chapter 11:** Notification to data subjects
- Information Regulator *Guidance Note on Processing of Personal Information of Children*, available at **https://inforegulator.org.za/wp-content/uploads/2020/07/GuidanceNote-Processing-PersonalInformation-Children-20210628-1.pdf**
- European Data Protection Board Statement 1/2025 on Age Assurance, 12 February 2025, available at **https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-12025-age-assurance_en**.
- European Commission Minimising the risks children and young people face online, 14 July 2025, available at **https://commission.europa.eu/news-and-media/news/minimising-risks-children-and-young-people-face-online-2025-07-14_en**.
- European Data Protection Board CEF 2026: EDPB launches coordinated enforcement action on transparency and information obligations under the GDPR, 19 March 2026, available at **https://www.edpb.europa.eu/news/cef-2026-edpb-launches-coordinated-enforcement-action-on-transparency-and-information_en.**
- Information Commissioner's Office Children's code strategy progress update – August 2026, available at **https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/children-s-code-strategy-progress-update-august-2026/**.

juta

© Juta and Company (Pty) Ltd. All rights reserved.