CIPL's Response to ANPD Consultation on the Draft Guidelines on "Age Verification Mechanisms"

Submitted 8 July 2026

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to contribute to the ANPD's public consultation on the Draft Guidelines on Age Verification Mechanisms ("*Mecanismos de Aferição de Idade*") published May 2026 ("the Draft Guidelines").[2]

CIPL commends the ANPD for a thoughtful, evidence-informed, and risk-based draft. In particular, we welcome:

- the recognition that age verification "is not an end in itself" but rather one pillar of a broader protective ecosystem;
- the structuring of the framework around proportionality and a risk taxonomy;
- the clear preference for privacy-preserving methods, including verifiable credentials, age tokens, double-blind architectures, and zero-knowledge proofs; and
- the emphasis on interoperability and data minimisation.

These positions are aligned with CIPL's extensive body of work on children's data privacy and age assurance.

Rather than responding sequentially to each section of the Draft Guidelines as structured in the consultation, CIPL has organised this response around the core principles and considerations that we believe should guide the development of an effective, proportionate, and child-centred framework. In particular, we draw on our contributions to the field of children's data privacy and age assurance[3]

---

1 **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 80+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at https://www.informationpolicycentre.com/. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

2 Agência Nacional de Proteção de Dados (ANPD), "Guia orientativo—Mecanismos de aferição de idade," public consultation, Brasil Participativo, available at https://brasilparticipativo.presidencia.gov.br/processes/Guia-orientativo-mecanismos-de-afericao-idade/f/4604/.

3 Since launching its Children's Data Privacy Project in 2021, CIPL has placed age assurance at the center of its research and policy engagement. Relevant work includes:

developed over several years through dedicated research, multistakeholder engagement, and regulatory consultation responses across multiple jurisdictions. We hope that these cross-cutting observations, summarised below, will be useful to the ANPD in refining the Draft Guidelines as a whole.

As a general observation and to ensure that the Guidelines' advisory character is reflected consistently throughout, we would recommend that the ANPD, where relevant, clearly distinguish between best-practice recommendations and obligations that flow directly from the law and the Decree.

No one-size-fits all solution

CIPL has consistently emphasised that there is no one-size-fits-all solution in age assurance: the appropriate mechanism, and the appropriate point in the user journey at which it is deployed, must depend on the nature of the service, the features and functionalities offered, and the likelihood and severity of the risks to children associated with that service.[4] Additionally, uniform approaches

- CIPL's 2022 Policy Paper, "Protecting Children's Data Privacy: International Issues and Compliance Challenges," which identified age assurance as one of the central compliance challenges relating to children's data;
- A series of Multistakeholder Dialogues on Age Assurance, held jointly with the WeProtect Global Alliance between 2024 and 2025, covering law and regulation, risk assessments, global and regional perspectives, and interoperability;
- A November 2025 paper proposing an Interoperable Framework for Age Assurance Solutions, exploring how interoperable, privacy-preserving credential architectures can support age assurance while safeguarding user autonomy;
- CIPL's paper on "Enabling Beneficial and Safe Uses of Biometric Technology Through Risk-Based Approaches," addressing safeguards relevant to biometric age estimation, including bias mitigation and liveness detection;
- Responses to consultations on age assurance and children's privacy frameworks in multiple jurisdictions. See https://www.informationpolicycentre.com/project/childrens-privacy/.

[4] Please see the takeaways from the Multistakeholder Dialogues on Age Assurance available on CIPL's website:

- Roundtable 1 (March 2024), available at https://www.informationpolicycentre.com/resources/a-multi-stakeholder-dialogue-on-age-assurance-key-takeaways/.
- Roundtable 2 (July 2024), available at https://www.informationpolicycentre.com/resources/key-takeaways-from-a-multi-stakeholder-dialogue-on-age-assurance-law-and-regulation/ .
- Roundtable 3 (September 2024), available at https://www.informationpolicycentre.com/resources/a-multi-stakeholder-dialogue-on-age-assurance-working-group-on-risk-assessments-key-takeaways-next-steps/ .
- Roundtable 4 (October 2024), available at https://www.informationpolicycentre.com/resources/key-takeaways-a-multi-stakeholder-dialogue-on-age-assurance-working-group-on-global-regional-perspectives/.

undermine children's evolving autonomy. Safety measures, including age assurance, should be tailored to specific age groups.

While the Draft Guidelines do rightly refer to progressive autonomy as a guiding principle, this is not translated into practical criteria that organisations can apply—for example, guidance on how default settings or protective measures should reasonably differ across age brackets. We would encourage the ANPD to develop such operational criteria and provide examples, so that the principle of progressive autonomy can be consistently applied in practice.

Risk based and proportionate approach

CIPL has consistently supported a risk-based and proportionate approach to children's privacy and safety: not all processing involving children's data presents the same level of risk, and measures such as age assurance, default settings, and design choices should be calibrated to the nature, context, and severity of the specific risk, as well as to the benefits of the processing.[5] Choosing a hard age verification method (such as document-based verification) where age estimation would suffice can result in disproportionate collection of personal data, including sensitive data, and may itself introduce privacy and security risks that outweigh the benefits to child safety. Conversely, relying on low-assurance methods in high-risk contexts fails to provide the protection the law requires. Equally, requiring full age or identity verification of all users across routine services without a consideration for risk would impose data-protection costs exceeding anything required offline, without

- Roundtables 5 & 6 (October–November 2024), available at https://www.informationpolicycentre.com/resources/key-takeaways-a-multi-stakeholder-dialogue-on-age-assurance-working-group-on-law-and-regulation/.
- Roundtable 7 (June 2025), available at https://www.informationpolicycentre.com/resources/a-multi-stakeholder-dialogue-on-age-assurance-considerations-towards-an-interoperable-age-assurance-framework/.

[5] Please see:

- A Multi-Stakeholder Dialogue on Age Assurance—Working Group on Risk Assessments: Key Takeaways & Next Steps, September 2024, available at: https://www.informationpolicycentre.com/resources/a-multi-stakeholder-dialogue-on-age-assurance-working-group-on-risk-assessments-key-takeaways-next-steps/ .
- Centre for Information Policy Leadership, "Response by the Centre for Information Policy Leadership to the OAIC's Consultation on the Children's Online Privacy Code," July 31, 2025, available at: https://www.informationpolicycentre.com/resources/cipl-response-to-the-office-of-the-australian-information-commissioners-office-oaic-consultation-on-the-childrens-online-privacy-code/.

commensurate evidence of a safety gain.[6] CIPL welcomes the Draft Guidelines' express attention to these considerations.[7]

We, therefore, strongly welcome the proportionality requirement in Article 24, I, of the Decree, and the risk matrix and illustrative case studies set out in the Draft Guidelines, which align the age assurance method to the risk level of the underlying service. [8]

In that same vein, where the applicable legal framework expressly exempts certain services from age assurance requirements, CIPL encourages the ANPD to clarify that such exemptions also extend to obligations to receive, process, or rely on third-party age signals. Otherwise, exempt services could face technical integration and data processing obligations that effectively replicate the age assurance measures from which they are exempt, undermining the very proportionality objectives of the Draft Guidelines and underlying regulatory framework. Clarification of this point would promote consistent implementation and avoid unnecessary compliance burdens for services subject to exemptions.

A Taxonomy of risks is crucial

As mentioned above, CIPL commends the ANPD for the development of the risk matrix and its accompanying examples of services and corresponding mechanisms across low, moderate, and high risk categories. In our work we have repeatedly observed that there is no broad consensus across jurisdictions on a taxonomy of risk or on the factors that should inform a risk assessment for age assurance purposes. The ANPD's risk matrix represents a valuable and concrete attempt to close this gap and provides organisations with a much clearer basis for determining which mechanisms are appropriate in which contexts.

Proportionality should genuinely permit lower-friction methods in lower-risk contexts. A clear, evidence-based risk taxonomy—supported by illustrative examples and case studies, especially for low- and medium-risk scenarios—is essential to avoid both under-protection (insufficient safeguards) and overprotection (disproportionate restrictions that limit access to beneficial content or that result in excessive data collection).

We would, however, encourage the ANPD to further develop the examples provided for the moderate risk category in particular. This category currently appears to cover a very broad range of services—from social networks and video platforms with mixed content, to generative AI services, digital health platforms, and general e-commerce—which differ significantly in terms of the nature and severity of

---

6 Joint Statement of Security and Privacy Scientists and Researchers on Age Assurance, March 2026, available at: https://csa-scientist-open-letter.org/ageverif-Feb2026.

7 ANPD Draft Guidelines, Section III (Proportionality) (adverse effects of the verification mechanism itself, which may affect both children and adults).

8 CIPL has consistently expressed this view in its consultation responses on children's privacy and safety. See, for example, "Response by the Centre for Information Policy Leadership to the OAIC's Consultation on the Children's Online Privacy Code," July 31, 2025, at page 13, available at: https://www.informationpolicycentre.com/resources/cipl-response-to-the-office-of-the-australian-information-commissioners-office-oaic-consultation-on-the-childrens-online-privacy-code/.

risk they may pose to children. More granular examples within the moderate-risk category, together with further guidance on how organisations should weigh the relevant risk factors in borderline cases, would help organisations apply the layered model consistently and would reduce the risk of divergent interpretations across the market.

Moreover, the ANPD may wish to consider that services operating in curated environments and with multiple safeguards—such as content classification, special child profiles, parental controls, and restricted viewing settings—can constitute examples of lower-risk services.

Recognising nuanced characteristics within the risk taxonomies and providing examples would support more consistent risk assessments and provide organisations with greater clarity when determining proportionate age assurance measures.

Additionally, the Draft Guidelines' risk matrix automatically classifies as high-risk *any service* offering content, products, or services prohibited to minors under 18. While the text identifies clear examples such as pornography, gambling, betting, or video games with loot boxes, the broad language referring to "*any service* … prohibited to minors" could be understood to encompass services that may not, in fact, present a high degree of risk.

For example, a vehicle rental platform may restrict bookings to adults, and some professional or B2B services may limit account creation to adults because of legal contracting requirements rather than concerns about harmful material. By automatically equating an 18+ designation with a high-risk classification, the Draft Guidelines overlook the broader range of factors that a Data Protection Impact Assessment (DPIA) should consider—such as the nature of the service, the actual risk arising from access as opposed to participation, existing safeguards, and the maturity of the user—in order to determine a proportionate and risk-based response.

Because the high-risk classification requires age-verification measures with a high degree of robustness, accuracy, and reliability—often involving government-issued identification or biometric verification—CIPL encourages the ANPD to recognise the need for a contextual risk assessment before requiring blanket age-verification measures to "*any service* … prohibited to minors."

CIPL would further encourage the ANPD to ensure that the risk taxonomy supports holistic, context-specific assessments that consider the full range of potential risks and benefits to children, beyond data protection impacts alone, with the best interests of the child serving as the guiding principle for regulatory and organisational decision-making. Such assessments should account for potential effects on children's access to information, inclusion, participation, and progressive autonomy, as well as the risk that disproportionate age assurance measures may exclude children from beneficial educational, cultural, and informational content. A balanced and holistic approach would better support proportionate, risk-based outcomes that protect children from harm while preserving their rights, opportunities, and ability to participate meaningfully in the digital environment.

The Role of Self-Declaration

CIPL supports the Draft Guidelines' position that self-declaration, on its own, does not constitute a sufficiently reliable age assurance mechanism for any higher-risk contexts. Self-declared information

without further corroboration is easily manipulated and therefore cannot provide the level of confidence required where a service presents meaningful risks to children's privacy, safety, or wellbeing.

At the same time, consistent with the proportionality principle described above, CIPL considers that self-declaration can have a legitimate, limited role where the risk associated with a product, service or piece of content is low—for example, where the consequences of an inaccurate age claim are negligible and where layering a more intrusive mechanism on top of self-declaration would itself be disproportionate. We would, therefore, encourage the ANPD to confirm that self-declaration may remain an acceptable starting point within the layered model specifically for low-risk contexts, while remaining clearly insufficient, on its own, for moderate- and certainly high-risk contexts as set out in the Draft Guidelines' risk matrix.

Risk Assessment should be continuous

CIPL believes that risk assessment must be continuous. What constitutes a risk—including a high risk—and what constitutes appropriate mitigation should be assessed on the basis of evidence and re-evaluated over time, as services evolve and our understanding of new risks and benefits evolves. A static understanding of risk can lead to either over or under protection with disproportionate data collection and verification requirements and potentially excluding users from beneficial services, while failing to protect them from emerging risks.

Ensuring that risk assessments remain accurate and continuous will further depend on organisations having clarity on the assessment tools available to them. We would encourage the ANPD to clarify how the DPIA recommended for moderate- and high-risk services relates to other impact assessments that may already apply to the same processing—such as the LGPD's data protection impact assessment, the ECA Digital's impact report, and the Decree's safety impact assessment—so that organisations know whether these are separate obligations or whether one assessment can satisfy several of them.

Best interests of the child to guide age assurance

Age assurance serves an objective beyond mere data protection; it supports comprehensive protection of children and adolescents in the digital environment. Age assurance advances not only their rights to privacy and safety, but it also affects their right to participate and express themselves through access to information, culture, digital participation, and the progressive development of autonomy.

Policy makers must therefore be mindful that age assurance does not merely become an exclusionary technology that blocks children from their benefits of the digital world. As mentioned above, overly rigid assurance requirements can lead to overprotection, where children are denied access to educational tools, social connectivity, and digital literacy resources that are fundamental to their development and participation in society. The deployment of age assurance tools must, therefore, be guided by the *best interests of the child* as the overarching north star, including the child's right to seek, receive, and impart information as guaranteed by Article 13 of the UN Convention on the Rights

of the Child,[9] as recognised in Brazil.[10] Age assurance should be understood as a gateway to age-appropriate experiences, not a mere barrier to entry.

Multi-layered and Interoperable solutions

Interoperability remains a key enabler of a privacy-protective ecosystem. As CIPL has supported in its multistakeholder dialogues,[11] interoperable approaches—including cross-recognition of credentials and convergence around international standards—reduce the need for repeated verification, lower compliance costs, narrow the surface area for breaches, and improve the experience for users, parents, and adults alike. CIPL therefore commends the ANPD for its support of international standards—including ISO/IEC 27566[12] and IEEE 2089.1-2024[13]—and further encourages it to promote convergence and reduce fragmentation for providers operating globally.

We also welcome the references to comparable international approaches such as the ICO's Age Assurance Children's Code (AACC).[14] CIPL has consistently stressed the value of regulatory convergence and coordination, particularly where similar concepts are deployed across jurisdictions.[15]

That said, we encourage the ANPD to provide clearer parameters on how the obligations imposed on both app stores and operating systems—in particular regarding the collection and transmission of age signals—should be operationalised in practice, how to address any conflicts between measures implemented by different app stores and operating systems, as well as the impact of practical technical limitations.

---

[9] United Nations General Assembly, Convention on the Rights of the Child, 20 November 1989, United Nations, Treaty Series, available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

[10] Decree No. 99,710, available at https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm.

[11] Centre for Information Policy Leadership, Considerations Towards an Interoperable Age Assurance Framework: Key Takeaways, available at https://www.informationpolicycentre.com/resources/a-multi-stakeholder-dialogue-on-age-assurance-considerations-towards-an-interoperable-age-assurance-framework/.

[12] International Organization for Standardization and International Electrotechnical Commission. ISO/IEC 27566-1:2025, *Information Security, Cybersecurity and Privacy Protection — Age Assurance Systems — Part 1: Framework*. Geneva: ISO, 2025, available at: https://www.iso.org/standard/88143.html.

[13] See IEEE Standard for Online Age Verification, available at https://standards.ieee.org/ieee/2089.1/10700/.

[14] Information Commissioner's Office. "Age Assurance for the Children's Code." Information Commissioner's Opinion, available at: https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/.

[15] See, e.g., Centre for Information Policy Leadership, "Response by the Centre for Information Policy Leadership to the OAIC's Consultation on the Children's Online Privacy Code," July 31, 2025, available at: https://www.informationpolicycentre.com/resources/cipl-response-to-the-office-of-the-australian-information-commissioners-office-oaic-consultation-on-the-childrens-online-privacy-code/.

As CIPL has also shown through our multistakeholder dialogues, age assurance involves multiple actors—including operating systems, app stores, identity providers, and online services themselves.

CIPL encourages the ANPD to avoid unnecessary duplication of compliance obligations where equivalent or appropriate safeguards have already been implemented by another participant in the value chain. For example, where a service has implemented effective, risk-appropriate age assurance measures, it should not necessarily be required to duplicate those measures by processing additional age signals obtained from third parties.[16]

Providing greater clarity regarding the interaction between different actors would promote legal certainty, reduce unnecessary compliance costs, and better reflect the proportionality principle that underpins the Draft Guidelines.

Incentivisation of PETs plays a central role

CIPL agrees that accuracy, robustness, and reliability are fundamental technical parameters for effective age assurance, but we emphasise that these requirements must always be balanced against privacy, data minimisation, and proportionality. For example, overprioritising absolute robustness and accuracy can also lead to the disproportionate collection of data, such as government IDs or high-resolution biometrics. To mitigate some of these tensions, CIPL has long encouraged the application of privacy-enhancing technologies (PETs) in the age-assurance context.[17] PETs can enable verification of a user's age without access to excessive personal data, thereby upholding the principles of data minimisation and privacy by design and by default.[18] CIPL, therefore, strongly welcomes the Draft Guidelines' emphasis on data minimisation and on privacy-preserving architectures based on

[16] The CIPL/WeProtect Interoperable Framework for Age Assurance Solutions asks for practical, flexible guidance for regulators that "recognises that companies' good faith efforts to address appropriate age assurance on their services should be supported if they offer adequate protection without forcing companies to adopt new approaches." Please see the Framework here: https://www.informationpolicycentre.com/resources/a-multi-stakeholder-dialogue-on-age-assurance-considerations-towards-an-interoperable-age-assurance-framework/.

[17] This is also supported by the EDPB in its Statement 1/2025 on Age Assurance: "[T]he EDPB recommends that, based on the state of the art in age assurance at the time this document was prepared, due consideration is given to technologies and architectures favouring user-held data and secure local processing (device-based), allowing properties such as unlinkability (from different parties' point of view and even in the case of collusions or data breaches) and selective disclosure of personal data under the control of the data subject. In addition, the use of approaches such as those relying on batch issuance of single-use credentials or cryptographic protocols such as zero-knowledge proofs should be made available for the data subjects in cases where age assurance may involve high risks to their privacy." European Data Protection Board, *Statement 1/2025 on Age Assurance*, adopted February 12, 2025, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-12025-age-assurance_en.

[18] Centre for Information Policy Leadership, Reconciling AI with the Data Minimization Principle: Bridging the Innovation and Privacy Gap, December 2025, available at https://www.informationpolicycentre.com/resources/reconciling-ai-with-the-data-minimization-principle-bridging-the-innovation-and-privacy-gap/.

verifiable credentials, cryptographic age tokens, and zero-knowledge proofs.[19] This aligns also with our work on an Interoperable Age Assurance Solutions Framework.

At the same time, CIPL would encourage the ANPD to make equally clear that the Guidelines remain technology-neutral overall and do not prescribe or implicitly favour any particular technical solution, provided the mechanism chosen meets the applicable standards of accuracy, robustness, reliability, proportionality, and data protection. An outcome-based approach to age assurance will accommodate technological innovation, avoid potentially disenfranchising new services, and allow providers to select solutions best suited to the specific risks of their services.

CIPL also supports the Draft Guidelines' recommendation on the implementation of technical and organisational safeguards on retention, secondary use, traceability, and sharing. However, we would encourage the ANPD to clarify that such measures are to be applied in a contextual, risk-based, and proportionate manner. Requirements addressing deletion or restrictions on further processing should be carefully calibrated so as not to foreclose processing that is reasonably anticipated and that serves the child's best interests, where supported by appropriate governance and oversight. In particular, rules on immediate data elimination and purpose limitation should leave room for retention strictly necessary to detect circumvention and fraud, support bias mitigation and accuracy calibration, and demonstrate compliance, provided such uses remain instrumental to the assurance system's protective purpose.

CIPL further encourages the ANPD to consider the use of regulatory sandboxes, where businesses and regulators can co-develop and test privacy-preserving age assurance models for accuracy and effectiveness before wider deployment.[20]

Conclusion

Overall, CIPL supports the ANPD's approach and appreciates the continued, consultative engagement with stakeholders. CIPL encourages ANPD to continue work towards an approach that:

- is risk-based and proportionate, with continuous re-evaluation and a clear, example-driven risk taxonomy;
- relies, wherever sufficient, on age-range or attribute detection rather than exact age or identity, and avoids subjecting adults to disproportionate verification;
- prioritises privacy-preserving methods and privacy-enhancing technologies, including verifiable credentials, age tokens, zero-knowledge proofs, and double-blind architectures;

[19] ANPD Draft Guidelines, Section III (Privacy and Protection of Personal Data); Article 24, III–VIII, and Article 24, § 3, of the Decree.

[20] Centre for Information Policy Leadership, "Learning from Practice: Designing Effective Regulatory Sandboxes," October 2025, available at https://www.informationpolicycentre.com/resources/learning-from-practice-designing-effective-regulatory-sandboxes/.

- promotes interoperability and international convergence, including alignment with recognised technical standards;
- treats the best interests of the child as encompassing the benefits of digital participation, not only protection from harm.

CIPL stands ready to engage further with the ANPD on any of the issues raised in this response, including through bilateral discussion, workshops, or participation in CIPL's ongoing Multistakeholder Dialogue on Age Assurance, and to contribute to subsequent consultations on the implementation of the Digital ECA and the Decree. We will also share relevant future work product, such as our upcoming work on AI-supported age estimation.