Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

WeProtect GLOBAL ALLIANCE


# A Multi-Stakeholder Dialogue on Age Assurance

## Key Takeaways

# Key Takeaways
# A Multi-Stakeholder Dialogue on Age Assurance

Day 1 | Tuesday, 26 March 2024 - Day 2 | Wednesday, 27 March 2024

## Evidence Based - Child Informed - Risk Based

Digital age assurance is a complex and sensitive issue, requiring a careful balancing of rights and risks. We sought to bring together experts from across a range of sectors to understand the current state of play - challenges and opportunities - and to advance a holistic and principles-based approach. Attendees represented a diverse range of organisations, including child rights, privacy, safety, academia, regulators, civil society and industry representatives from technology, entertainment, telecommunications and financial sectors.

The event was held under the Chatham House Rule. Below is a summary of the key points of discussion, as well as a call for expressions of interest in participation in ongoing working groups.

## Age Assurance

- Age assurance is an umbrella term which includes age verification (identity documents, parental consent etc.) and age estimation (age inference, based on behaviour on a platform, social vouching, AI-based facial age estimation).
- It is widely recognised that self-declaration alone is generally inadequate as a means to help higher-risk services identify the user's age (apart from when used in addition to other methodologies).
- It is key to realise that services have very different challenges that manifest at different stages of their users' journey.
- Age assurance should be seen as a process, not a one-off check.
- Getting age assurance right is important. However, it is not a panacea and must not distract from other legal compliance and accountability activities that organisations need to put in place to ensure online safety and privacy in the delivery of their products and services to children.

## Striking a Balance between Safety and Privacy

- When implementing age assurance solutions, organisations must consider the appropriate balance between safety and privacy. Age assurance is part of digital safety by design, but solutions must also come from a privacy by design approach.
- Data minimisation, storage limitation, and data security must be balanced against the necessity to process data in line with the perceived risk. It is imperative that those responsible for safety, security and privacy within organisations cooperate to determine the appropriate balance.
- Any approach must be mindful of the difference between privacy and safety and the need to address both privacy and safety interests and rights: there may be one privacy concern versus many safety ones we are trying to solve when we contemplate age assurance solutions.
- Red teaming and starting with a "what could go wrong" approach to designing age assurance solutions is critical.

## The Regulatory Landscape

- Legal and regulatory fragmentation remains a major concern for many organisations.
- Broad global landscape of diverging child privacy and safety legislation, including age assurance and verification requirements, is creating challenges for international organisations.
- Regulatory guidance is available and being developed especially by European regulators (including the UK) for both privacy and safety, which should help to establish more legal clarity.
- More institutionalised cooperation between different regulators in Europe (including from different disciplines) and internationally is imperative to reach a level of convergence that ensures consistency in the protection of children online.
- Models such as the Digital Regulation Cooperation Forum in the UK and other nascent fora are extremely important to support a consistent approach, including by supporting the development of joint privacy and safety guidance and shared regulatory expectations.

In turn, regulators expect better assessments of risks and harms from organisations. When it comes to age assurance solutions in particular, companies must be able to demonstrate the effectiveness of age assurance solutions in the context of their service. Organisations must be ready to provide evidence of how solutions mitigate the assessed risk and the efficacy of the measure.

## Importance of a Context-and-Risk-Based Approach

- There is no “silver bullet” or proportionate “one size fits all” solution that could be deployed for age assurance that could satisfy all privacy and safety needs. The deployment of age assurance should follow a risk-based approach and solutions must be based on the issue we are trying to solve and the context and the type of services and products offered to children.

- There is no consensus on the risk taxonomy in general when it comes to digital policy and compliance. However, when it comes to assessing risk in the deployment of age assurance solutions, it is important to consider the benefits, in the context of the best interest of the child.

- Any risk assessment must be context specific and consider both the likelihood and severity of a risk of harm.

- High risk lists, which set out instances where a greater risk to children is likely, should be rebuttable and we should consider integrating risk assessments across the various legislations to facilitate operationalising them.

- Age assurance measures must be proportionate to the level of risk on a particular service and not collect more data than is necessary. Furthermore, as services develop and the environment changes over time, risks will change. This means risk assessments must be systematic and repeatable.

- Different stakeholders must work together to create holistic and contextual risk assessment frameworks that incorporate human rights, child rights, data protection and safety that translates into demonstrable measures.

- Adherence to existing and developing codes and standards can lower the overall risk for children on a platform or service and minimise the necessity for age assurance measures.

## Technical Challenges and Opportunities

- The question of 'reuse'/'interoperability' is a continuing point of discussion. Sharing signals and information is one approach to age assurance. If users can successfully verify themselves in one digital place can trusted providers hold the verification keys? This exists in other areas (telecoms, ID providers) – can this be extended to age assurance solutions?

- Such an approach may require further guidance also from regulators on data sharing and liability questions.

- Privacy-enhancing technologies, in particular zero knowledge proofs as suggested by the CNIL in France, may play a future role. Regulators should incentivise development and adoption of PETs.

- There is space for age assurance providers, but also a space for more development by platforms. Stakeholders should develop a roadmap for technological advances (AI for age assurance).

- There has to be an understanding, especially from privacy regulators, that the more granular and specific the age verification, the more (personal) information may have to be processed (children often lack ID for instance).

- There is further need to reconcile a layered approach to age assurance with the views expressed by some parents, children, and young people that there are "too many hoops to jump through" and experiences across different apps to verify age.

## User Experience and Education

- Age assurance and parental control tools must be accessible to children, young people and parents. Bringing them along the privacy, security and online safety journey, and ensuring user-centred and participatory co-design is part of accountable and responsible technology behaviour.

- While the responsibility lies with the organisations, there is a role for parents – and children and youth in peer-to-peer support – and we need to build their capacity and understanding. Making available controls, assurance and guidance in a single place via tools which parents and children already access and are familiar with, would help with this.

- All children and parents' perspectives or means are not the same however and the challenge lies in differing attitudes to parental controls and age assurance that can vary across age, culture and socio-economic status.
- There is a need to continuously ensure that product developers are up to date on child rights frameworks, legal requirements and child friendly design. Diverse teams that include children can ensure that teachable moments (such as when somebody gets rejected by age assurance) come with the right message to further the understanding of why certain measures are in place.
- Part of the approach to online safety must also be to incentivise children and young people to remain on the age appropriate pages.
- Schools often lack resources to provide the necessary media literacy education (focused on stranger danger).

## Ethical and Other Considerations

- Age assurance must be equitable, privacy and security minded.
- Ethics require organisations to consider "should we do this?", as well as "what if we don't do this". A benefit to many may override a risk to few.
- Rights-based language and frameworks form the cornerstone of age assurance principles.
- The process of standard-making needs to be much more inclusive – large portions of the world remain undocumented, and barriers to inclusion for CSOs remain very high in some countries as an example.
- How do we adapt approaches for those who have different needs based on socio-economic status, disability, familial structure and many other markers of difference?
- Suggestions to rethink the 'magic number 13' and whether other age bands relate to developmental needs for children and teens.
- We should consider who we mean when we refer to "the child" – the term reflects different realities in different jurisdictions.

## Action Points and Next Steps

As a next step, we plan to set up a number of smaller dedicated working groups on the following topics:

- **Law and regulation**: to consider relevant legal and regulatory frameworks in the international context, including suggestions for where greater legal clarity is needed, potential challenges (e.g., overlap, conflicting proposals, different roles of companies in the age assurance ecosystem), and opportunities to advance interoperable age assurance.

- **Risk assessments**: to explore the role of risk assessments in supporting a balanced and rights-based age assurance and the opportunities to develop a more holistic approach to assessing both safety and data protection risks to young people and consider both risks and benefits.

- **Regional and global perspectives**: to gather international insights on age assurance, including regional, cultural and socioeconomic factors that may require variations, and assess lessons learned for a global approach.

- **Future mapping**: to explore and map emerging activities relating to age assurance, including the development of standards, technology and partnerships.

These four groups will meet virtually and will seek to gather insights from a variety of experts. They will produce a short paper (or other relevant output) setting out their discussions and learnings, drawing on the foundations of the March roundtable in London.

If you are interested in joining one of these working groups, please contact Natascha Gerlach (NGerlach@huntonak.com) and Eden Tayyip (ETayyip@huntonak.com) or Iain Drennan (Iain@weprotectga.org) by **Friday, May 31, 2024**.

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

WeProtect GLOBAL ALLIANCE

# **A Multi-Stakeholder Dialogue on Age Assurance** Law and Regulation


## Key Takeaways

# Key Takeaways
# A Multi-Stakeholder Dialogue on Age Assurance - Law and Regulation

Brussels, Thursday 11th July 2024

The Centre for Information Policy Leadership (CIPL) and the WeProtect Global Alliance are continuing their efforts to promote a global dialogue involving multiple stakeholders on age assurance. Following a successful two-day meeting in London in March, CIPL and WeProtect continued their efforts in a second of a series of in-person and virtual events on age assurance held in Brussels on July 11th, 2024.

Following the London event, four discrete working groups were formed to enable a more focused discussion and drive the development of consensus-based principles that can ultimately also inform the wider policy discussion.

This second multi-stakeholder dialogue also served as the inaugural meeting of the law and regulation working group. The discussion was grouped around three main topics:

- **The When:** A risk-based approach to age assurance
- **The What**: Defining state of the art and finding a common baseline among differing age assurance mechanisms
- **The Who:** Roles and responsibilities in age assurance

Attendees represented a diverse range of organisations, including child rights organisations, academia, privacy and safety regulators and experts from a number of jurisdictions, lawmakers, government representatives, civil society, age assurance providers, and a wide range of industry representatives including the technology, adult entertainment, social media, telecommunications and financial sectors. The event was held under the Chatham House Rule.

The insights gathered from this session will feed into follow up meetings of the working group. More information on the working groups and how to take part can be found at the end of this summary.

Below is a high-level summary of some key areas of discussion.

# The When: A risk-based approach to age assurance

## Risk Assessments - Balancing Privacy and Safety

Navigating risk assessments is undeniably complex and made more complex by the increasing number of laws governing various aspects of children's online experiences. Guidance regarding risk assessments under the GDPR is available, and guidance regarding safety laws such as the Digital Services Act or the Online Safety Act is still emerging.

- Some organisations continue to struggle to construct meaningful risk assessments and effective mitigation measures in this cross- sectoral environment. For instance, risk in the context of processing under the GDPR will differ from risk in the context of content as do the corresponding mitigation measures. New risk terminology such as “systemic” risk is not as well defined yet. Understanding the risk and defining appropriate mitigation measures therefore remains an iterative and continuous process.

- At the same time, organisations must carry out risk assessments carefully and honestly. Frequently risks are flagged to be medium or low risk where in reality they present a high risk profile.

- Where assessing risks it is important to avoid conflating different types of risk (such as the 4 Cs), and to ensure that risk is viewed in contexts including where risk may be created by other children.

- Age verification measures may need to be weighed against the potential benefits of access to content like LGBTQ+ resources, in particular as children move through maturity levels.

- The Best Interest of the Child must be considered when determining what makes a service age appropriate. However, more clarity is needed in terms of what constitutes the Best Interest of the Child. The understanding of what constitutes the Best Interest of the Child may differ across jurisdictions and in different cultural contexts and even from one child to another. It is challenging to explain this concept to product teams but standards such as the UN Convention on the Rights of the Child General Comment 25 (relating to rights in the digital world) provide valuable insights.

- Creating appropriate and practicable risk assessments will require a cross functional approach including C-Suite involvement, legal, content specialists, product teams, privacy and safety experts. This has to translate into internal accountability measures such as appropriate policy and procedures and training to support sufficiently holistic risk assessments and the development of effective risk mitigation measures. Having a multi-disciplinary team that has a consistent dialogue to convene on safety decisions, edge cases and product cases is also important.

- Regulatory cooperation, nationally and ultimately internationally, is key to creating a common understanding and a coherent approach to guidance and enforcement as demonstrated in the UK under the DRCF. Similar developments are emerging in other jurisdictions such as the Netherlands, Ireland and Germany.

- The development of standards, nationally and internationally, can further support a balance of innovation and safety across global platforms while creating a level playing field for assessing risk. However, an agreement has to be reached as to how specific standards should be.

# The What: Defining state of the art and finding a common baseline among differing age assurance mechanisms

## Defining 'State of the Art' and technical solutions

In Europe the discussion around age assurance often centers around Article 8 of the GDPR, and consent. This has commonly led to platforms and services with child users having terms of service which require users to be 13+. Whether motivated by the GDPR, DSA, OSA, AVMD, or existing age appropriate design codes, any age assurance measure must be proportionate to the context in which it is deployed and must be weighed against the best interest of the child including the right to play and for children to express themselves. Other considerations include whether the solution is sufficiently privacy friendly, secure, and designed in a manner that is easy to understand and use.

- While there is generally agreement that age assurance will not have a one-size fits all solution, determining what could be considered a “state of the art” baseline could provide a level of consistency for regulators and organisations alike.

- The GDPR makes reference to "state of the art" throughout but does not define it in order to remain appropriately tech neutral. Frameworks from other sectors working with the concept of "state of the art" such as ENISA's three step process for IT security can provide helpful learnings, however: State of the art age assurance measures should be commercially available, consider existing scientific knowledge and generally accepted rules or standards, and must move away from deprecated approaches that are known to be less effective or compromised. As an example, self-declaration at least when used without any supplemental measures, is unlikely to be acceptable as state of the art anymore, where age assurance is mandated. Other approaches such as social vouching are still being evaluated.

- Age assurance technology must take the different age bands of children and teens into consideration and the challenges that this may bring. For example, some technologies while generally commercially available, such as using payment information or digital ID solutions, may not be available for the 13+ age band for instance.

- New methods, such as voice age estimation, are a developing area and have the potential to become 'state of the art'. This requires room for innovation and a continuous evaluation process by organisations and regulators alike.

- Organisations operating globally face the challenge that not all age assurance measures will be accepted in every jurisdiction; as an example age verification solutions based on biometrics are approached differently across EU member states, or in the US.

- Cultural differences and different national cultural contexts (e.g., varying parenting approaches and different perceptions of harmful content) have an impact on the uptake of age assurance technology. This may require to make allowances for local specificity, but should not lead to drastic divergence across jurisdictions either. Technical solutions must be tested in the real world and testing must involve children and parents in the design.

- Additionally, good practices can be drawn from experience in other sectors with access limitations such as in the insurance or banking sector, alcohol or gambling industry and successful cross-sector collaboration such as between tech platforms and the alcohol industry.

- Privacy remains a major concern for the implementation of effective age assurance mechanisms and finding the right balance between the various trade-offs can be a challenge. Privacy-enhancing technologies (PETs) including AI-based technologies can provide mitigation measures.

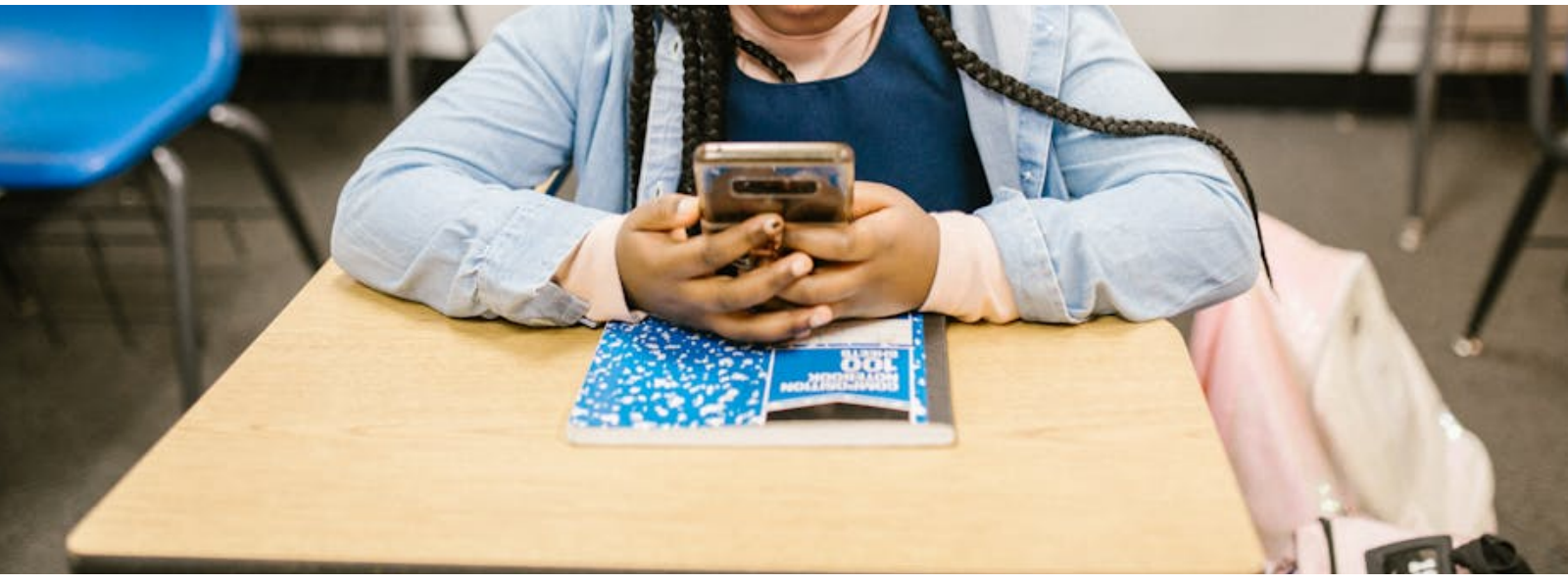
# The Who: Roles and responsibilities in age assurance

## Device, service, platform and parental responsibility

Parents, caregivers, and also children have agency and an important role to play in the context of effective age assurance. Parents can play a key role in protecting their children. In reality families and caregivers are often overwhelmed by the volume of interactions with different individual services and the technical knowledge this involves. To be effective, age assurance measures (and parental control tools) should strive to be user-friendly and easy to understand, including by children.

- Solutions for age assurance involve different actors in the online ecosystem from the telecommunications providers, to the online platforms, device manufacturers, app stores, and individual apps. Proposals to streamline the process for the benefit of users include browsers, app stores or device OS as opportunities to establish age at a central point of contact, which has the advantage of building on some already existing infrastructures. However, such an approach would need to carefully balance a number of challenging issues including privacy, security, competition concerns, costs and liability. Experiences in the US also raised questions around sufficient granularity of such an approach given the exclusionary nature of age assurance. Workable solutions will have to carefully address all these concerns.

- Overall, all efforts should be made to align policy and legislative approaches wherever possible and diverge only when necessary. With principle-based laws and a risk-based approach, there will always be a degree of ambiguity which is to be embraced to remain tech neutral. It relies on organisational accountability and an iterative process of developing appropriate policies and tools to respond to developing risks. It is also an opportunity to align through multi-stakeholder initiatives such as this on some of these issues and inform future approaches.



# Recommendations and Next Steps

## Proposed Recommendations

**1.** Develop a framework: Establish an inclusive framework for the when, what and who of age assurance. This should be developed involving multiple stakeholders and follow a principle- and risk-based approach, taking account of key global laws and regulations.

**2.** Promote collaboration: Encourage ongoing collaboration between organisations, regulators, industry, and international bodies.

**3.** Enhance guidance: Develop guidance for product and design teams on child privacy, safety and security and associated risk assessments, which could be reinforced by training programmes. A culture of compliance and training should also be built for parents, guardians and children.

**4.** Innovate safely: Leverage new technologies for effective age assurance while protecting privacy by undergoing a continuous evaluation process and define clear standards.

**5.** Engage stakeholders: Involve parents, educators, and children in developing and implementing an age assurance framework, with a key focus on child participation.

# Next Steps

## Working Group Membership

To continue the exchange and work through the complexities of these issues, a series of working groups are being established to further this initiative. The aim of the working groups is to facilitate discussion and progress on each of the below work streams, providing the opportunity to gather further insights from a variety of experts and perspectives.

The three working groups are:

### Law and Regulation

Terms of reference - *To consider potential framework(s) for the implementation of age assurance under European relevant laws and regulations, with a view to this knowledge being applicable to other global regions. This will take account of potential challenges (e.g., overlapping laws, conflicting viewpoints and regulator perspectives, different roles of companies in the age assurance ecosystem) and opportunities to advance interoperable age assurance.*

### Risk assessments

Terms of reference - *To explore the role of risk assessments in supporting a balanced and rights-based age assurance and the opportunities to develop a more holistic approach to assessing both safety and data protection risks to young people.*

### Regional and global perspectives

Terms of reference - *To gather international insights on age assurance, including regional, cultural and socioeconomic factors, and assess lessons learned for a global approach.*

Each working group will meet virtually for 90 minutes on up to two occasions before the end of 2024 and will produce a short summary paper of key discussions and learning. All groups will receive secretariat support from Praesidio Safeguarding, who will coordinate the logistics of meetings, compile minutes and produce a draft summary position paper for each working group, which will be reviewed by working group members. Participation in the working groups is voluntary and not an endorsement of the paper or the wider project.

If you would like to be involved in this work and in shaping the outputs and recommendations for one or more of these groups, please contact Natascha Gerlach (ngerlach@huntonak.com), Iain Drennan (iain@weprotectga.org), Eden Tayyip (etayyip@huntonak.com), and the secretariat support for the working groups (AgeAssurance@praesidiosafeguarding.co.uk).

All expressions of interest should be received by **30th August 2024**

# Who We Are

**CIPL** is a global privacy and data policy think and do tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world.

**WeProtect Global Alliance** brings together over 300 members from governments, the private sector, civil society and intergovernmental organisations to develop policies and solutions to protect children from sexual exploitation and abuse online. WeProtect Global Alliance is registered as a Stichting (foundation) in the Netherlands, with a subsidiary company registered in the UK. A Global Policy Board provides expertise and advice to monitor and guide the activities of the organisation.

**Secretariat support: Praesidio Safeguarding**

Praesidio is a specialist child online safety consultancy that believes that every child has a right to be safe and to thrive in the digital environment. Praesidio is committed to delivering high quality projects which help to create a better and safer online experience for children and young people.

Additional support provided by Microsoft, Snap and TikTok.

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

WeProtect GLOBAL ALLIANCE


# A Multi-Stakeholder Dialogue on Age Assurance

## Working Group on Risk Assessments

## Key Takeaways and Next Steps

Working Group Meeting, 19 September 2024

# A Multi-Stakeholder Dialogue on Age Assurance

## Working Group on Risk Assessments

KEY TAKEAWAYS & NEXT STEPS

19 September 2024

Brussels and Online

As part of the ongoing multi-stakeholder dialogue on age assurance led by the Centre for Information Policy Leadership (CIPL) and the WeProtect Global Alliance, the Working Group on Risk Assessments held a hybrid meeting on 19 September 2024 under the Chatham House Rule.

The aim of the meeting was to further the understanding of the complexities and challenges of assessing risk—specifically in the context of whether and how to deploy age assurance methodologies—and to outline a framework for a robust risk assessment that takes privacy and safety considerations into account.

Below is a high-level summary of the key takeaways, along with suggested next steps.

## KEY TAKEAWAYS

### Identifying Current Challenges

- The risk assessment landscape remains challenging due to varied and yet undefined terminology (e.g., "systemic risk") across different regulatory regimes. Moreover, similar terminology can mean different things in different cultural contexts, adding to the complexity. Stakeholders need a clear baseline for risk assessments, with a focus on the risk of *what*, to *whom*, and *when*, and the best interests of the child as the guiding North Star.

- Risk assessments in the context of the GDPR differ from risk assessments in the context of children's safety. Risks also vary in the context of different online services and their offerings.

- Regulators and regulated entities may understand and categorize risks differently, with regulators often attaching a higher risk score.

- Companies continue to struggle when addressing pertinent risks comprehensively. Holistic risk assessments require consideration of a number of issues, including human rights, children's rights, data protection, and safety. A holistic approach requires engagement with all relevant stakeholders early in the risk assessment process.

## Overarching Considerations

- A one-size-fits-all approach is insufficient; a contextual assessment of risks and opportunities is essential.
- Risk assessments should be forward-thinking to account for emerging risks, such as those presented by AI.
- In light of rapid product development and continual upgrades of product features, risk assessments should be iterative and flexible, incorporating specific mitigation strategies to unique risk profiles and tailoring age assurance solutions to specific services and offerings. The best solution may sometimes comprise a combination of different approaches.
- Meaningful assessments start with a clear understanding of the severity, likelihood, and type of risks for a given product or service.
- Assessments should evaluate specific objectives, such as safeguarding children from inappropriate content and preserving the right to freedom of expression.
- Establishing a baseline for risk assessments can help industry identify shared risks and ensure consistency when deploying age assurance methodologies. Sharing proposed best practices based on multistakeholder engagement will advance the discussion.

## Balancing Safety and Privacy

- Some companies segregate privacy issues from safety issues, but in the context of deploying age assurance technologies, privacy and safety teams should cooperate to ensure a holistic risk profile.
- Privacy risks and safety risks should be addressed holistically to ensure the protection of children's data and accessibility of age-appropriate content in an accountable manner.

## Implementing Accountability and Governance Measures

- Robust accountability measures—with a clear understanding of the decision-making process and internal responsibilities—will ensure that risks are appropriately addressed and mitigated.

## Embedding Risk Assessments into Product Design

- Risk assessments should not be a one-time exercise, but an iterative, flexible process. Ideally, risk assessments should already be embedded at the product design, user experience design, and product testing stages to ensure full consideration of safety and privacy issues as early as possible. This should include ethical considerations—such as "*Should we do this?*" and *"What happens if we don't?"*.

- Risk assessments should consider the impact of emerging technologies and potential enhancements to product features, ensuring that age assurance tools remain applicable and appropriate to evolving digital ecosystems. Those responsible for assessing risk should collaborate with product teams and technology developers to understand what innovations (and potential new risks) are on the horizon and to ensure that new factors are considered.

- An organization's approach to defining risks should also adapt as technologies evolve. Organizations will need to determine how to assess potential risks posed by technological enhancements and how to amend the organization's risk framework accordingly.

- Organizations should consider providing guidance for engineers and technologists to help prioritize the safety, privacy, and developmental needs of children through a structured approach to designing age-appropriate online environments (e.g. the CEN-CENELEC Workshop Agreement on an Age-Appropriate Digital Services Framework).

### Balancing Age Assurance with Children's Rights and Participation

- Organizations should factor in potential privacy risks associated not only with the collection and processing of children's data when using age assurance measures, but also the data of adults who may be required to provide proof-of-age to access material deemed inappropriate for children. Recent accounts of the hacking or sharing of users' data have brought to light some of these potential concerns.

- Organizations should take into account the possibility that certain age assurance measures may exclude some adult users from services or platforms that they otherwise have the right to access and, in certain cases, may impair the ability of minors and children to access and participate in age-appropriate services and platforms.

- Organizations should reassess the effectiveness and appropriateness of age assurance measures over time, taking into account the developmental and maturity level of children as they grow older.

- As with any risk assessment, organizations should factor in the benefits and opportunities related to age assurance measures, along with the risks. Age assurance has the potential to enable the creation of specialized services for specific age groups that only members of that age group can access. The potential benefits of such a service should not be lost in the conversation about risks.

### Incorporating Children's Perspectives

- Children's input should not be overlooked when designing and implementing appropriate age assurance measures. Young people of different ages can offer unique perspectives and valuable feedback on the ease, effectiveness, and utility of a given methodology—all of which should be considered for a truly holistic risk assessment. Equally, children's increasing autonomy and maturity levels should be taken into consideration, and risk assessments

should consider cultural, familial, or even government contexts that could touch upon privacy or safety concerns (e.g. in an LGBTQ+ context).

- Finally, parental/care-taker involvement is equally crucial. Educators also play a role and their perspectives should be reflected. Designing appropriate age assurance measures should take these considerations and relationships into account, with an understanding of regional and culturable differences and sensibilities.

## AVAILABLE RISK ASSESSMENT GUIDANCE

- U.K. Information Commissioner's Office: Children's Code Self-Assessment Risk Tool
- U.K. Office of Communications (Ofcom): Quick guide to children's risk assessments: protecting children online
- U.K. Digital Regulation Cooperation Forum (DRCF): A Joint Statement by Ofcom and the Information Commissioner's Office on Collaboration on the Regulation of Online Services
- European Union: BIK [Better Internet for Kids] age assurance self-assessment tool for digital service providers
- Ireland Data Protection Commission: Fundamentals for a Child-Oriented Approach to Data Processing

## SUGGESTED NEXT STEPS

- **Develop an overview of risks and guidance.** Create a mapping of existing regulatory frameworks and risk assessment tools to include specific features and types of risk to be assessed across different services.

- **Define tangible mitigation measures.** Propose practical examples of risk assessments and real-world application case studies to help smaller organizations navigate compliance.

## WHO WE ARE

**The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure 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 of the law firm Hunton Andrews Kurth LLP. This document is not designed to be and should not be taken as legal advice.

**WeProtect Global Alliance** brings together over 300 members from governments, the private sector, civil society, and intergovernmental organisations to develop policies and solutions to protect children from sexual exploitation and abuse online. WeProtect Global Alliance is registered as a Stichting (foundation) in the Netherlands, with a subsidiary company registered in the UK. A Global Policy Board provides expertise and advice to monitor and guide the activities of the organisation.

### Secretariat support: Praesidio Safeguarding

Praesidio is a specialist child online safety consultancy that believes that every child has a right to be safe and to thrive in the digital environment. Praesidio is committed to delivering high quality projects which help to create a better and safer online experience for children and young people.

# A Multi-Stakeholder Dialogue on Age Assurance

## Working Group on Global & Regional Perspectives

# KEY TAKEAWAYS

Working Group Roundtable

22 October 2024

Washington, DC

# A Multi-Stakeholder Dialogue on Age Assurance

## Working Group on Global & Regional Perspectives

KEY TAKEAWAYS

22 October 2024

Washington, D.C.

On 22 October 2024, the Centre for Information Policy Leadership (CIPL) and the WeProtect Global Alliance continued their multi-stakeholder dialogue on age assurance in Washington, D.C., where the Global and Regional Perspectives Working Group held its inaugural meeting. The in-person, invitation-only roundtable brought together representatives from industry, academia, and civil society to get a better understanding of the state of play of age assurance, with a particular focus on developments in the United States.

The event was held under the Chatham House Rule.

Below is a high-level summary of the key takeaways, followed by suggested actions.

## KEY TAKEAWAYS

- **Age assurance requirements in US state legislation address a diversity of harms.** US state laws requiring the use of age assurance have arisen in response to concerns about harms to minors from their use of the internet. However, there is no consensus among the states on the harms sought to be addressed. Some seek to shield minors from accessing pornographic content, others seek to prevent access to social media platforms, and still others seek to curb so-called "addictive feeds." Indeed, even laws purporting to address the same type of harm present different views of that harm. Nevertheless, all of the laws view age assurance as a means to curb the harm, whatever it may be.
- **Effectiveness of age assurance measures to mitigate harms is an open question.** Given that US state laws are still in their infancy, assessments on the effectiveness of age assurance measures to accomplish their varied goals do not yet exist. Notwithstanding the challenges raised by these laws—from both a legal (constitutional) perspective and a practical (implementation) perspective—state legislators will likely remain active in this area, continuing to view age assurance as a "silver bullet" to address a host of alleged harms—a view not shared by most of the participants, who recognize the need to use a combination of measures, not age assurance alone, to keep children safe online.
- **Risks to privacy from the collection of data.** While many state laws prohibit the retention of data collected for age assurance, participants nevertheless expressed concerns about potential risks

materializing prior to the deletion of such data, such as unauthorized data sharing, data harvesting, and potential secondary uses. The potential fallout from unauthorized access and related security incidents is a perennial concern.

- **Clarity is needed for action thresholds and knowledge standards.** State legislative measures can on occasion be vague on what triggers the obligation to use age assurance. Companies are sometimes unsure if they must independently assess the age of users *before* employing an age assurance method, especially in situations where the obligation arises in the case of a "known child" or a "known minor." For example, New York's Safe for Kids Act prohibits the operator of an "addictive social media platform" from providing an addictive feed to a covered minor unless the operator has obtained verifiable parental consent. Must an operator first determine if a user is a covered minor before deploying a consent feature? Relatedly, companies are sometimes unsure whether age assurance should be deployed to satisfy a "should have known" threshold in laws that do not expressly mandate the use of age assurance measures.

- **Industry standards and certifications can build trust in age assurance measures.** Participants recognize the benefits of age assurance technologies and appreciate third-party vendors' transparency in sharing data and findings that support their products. Participants noted the need for international industry standards and certifications to establish a baseline for vendor services, to enable benchmarking, and to build confidence in vendor offerings generally. Standards and certifications could also help varied stakeholders (e.g., lawmakers, policymakers, and the general public) to understand the capabilities of different technologies.

- **A variety of elements factor into an assessment of age assurance measures.** An assessment of the effectiveness of a given age assurance method depends on priorities and perspectives. Each method has different strengths and capabilities, and a measurement of its success will vary depending on the factors deemed most important, e.g., accuracy of the results, minimization of data collection, ease of use, etc. Sometimes these factors can be in tension. For example, an end-user taking a selfie while holding a government ID can provide highly accurate results, but it also collects a great deal of data. The key factors for assessing age assurance methodologies include:
    - **Privacy:** How privacy-protective (or privacy-invasive) is the methodology?
    - **Effectiveness:** How effectively does it assess or estimate age?
    - **Cost:** What is the cost of implementation for platforms?
    - **User experience:** To what degree does the methodology introduce unwanted friction or impose an undue burden on adults accessing legal content?
    - **Interoperability:** Will it work across all user platforms, or will it require frequent re-verification?
    - **Inclusivity:** Will it work appropriately for all users, or will it disproportionately generate erroneous results for some?

- **It's not too late to develop industry-led solutions.** Participants representing the alcohol and tobacco industries recounted how they were intentionally proactive upon entering the online marketplace by coalescing around a voluntary, industry-led standard, which curbed the need for regulatory action. While industries from other sectors are already facing age assurance laws and regulations, they can nevertheless be proactive in developing industry-led solutions to share with regulators. Still, industry players recognize that the formulation of such solutions will be challenging to build and adopt, given the different roles and responsibilities of stakeholders across

the online ecosystem. Stakeholders are not likely to align on a single approach. Flexibility will be key to advancing a range of solutions moving forward.

- **A risk-based approach may be in tension with political realities**. Participants generally agreed that age assurance measures should be appropriate and proportionate to the level of risk and not be overly prescriptive. Most would therefore support legislation that requires a risk assessment with a proportionate response (without overly prescribing what that response would be). That said, laws are being enacted without requiring risk assessments, as lawmakers have already deemed certain content or certain platforms as high risk. While some participants felt the need to push back against laws lacking an assessment of risks, others thought that support for particularly effective, privacy-protective forms of age assurance—rather than advocating for risk assessments—would be an easier lift, given the political pressure.

- **Special considerations around age assurance legislation.** Participants raised concerns about age assurance measures potentially leading to the suppression of certain types of speech or the chilling of anonymous speech. Although many state laws are currently being challenged in US courts, some feared that such laws could nevertheless be copied in countries that lack robust free speech protections. Moreover, to the extent certain laws include parental consent and/or parental control provisions, some cautioned that such features could inhibit minors' access to information and/or fora they deem valuable.

## SUGGESTED ACTIONS

- **Articulate age assurance capabilities clearly and transparently.** Stakeholders should develop a framework that articulates and clarifies different approaches to age assurance so that policymakers, legislators, industry, and others can understand the strengths and weaknesses of different methods and choose the method(s) best suited for a given purpose.

- **Evaluate whether and how age assurance effectively mitigates identified harms.** Evidence is needed to assess the effectiveness of age assurance in mitigating the harms sought to be addressed by legislation, since minors are quite savvy in fashioning technical workarounds. Relatedly, evidence is needed to measure the impact of various methodologies on minors' (and adults') access to certain content. Stakeholders should work together to devise a means to collect such evidence and share it with policymakers and legislators.

- **Develop industry standards and certifications.** International industry standards would help establish a baseline for vendor services, enable benchmarking, and build trust in the use of age assurance technologies. The draft international ISO Age Assurance standard would be a good starting point. Certifications by independent third parties should be explored in tandem.

- **Promote privacy-protecting and privacy-preserving solutions.** Limitations on the collection, use, sharing, and retention of data related to age assurance should be established and implemented in laws and regulations.

- **Endorse a proportionate, risk-based approach to using age assurance.** Future laws and regulations should adopt a risk-based approach, and current regimes should consider amendments supporting an approach that enables the use of age assurance measures appropriate to the risks that arise in a given context.

- **Evaluate the impact of age assurance provisions on marginalized communities.** Lawmakers and policymakers should be made aware of the potential impact of age assurance methodologies on marginalized or disadvantaged communities, such as those who may lack government-issued IDs.

## WHO WE ARE

**The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure 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 of the law firm Hunton Andrews Kurth LLP. This document is not designed to be and should not be taken as legal advice.

**WeProtect Global Alliance** brings together over 300 members from governments, the private sector, civil society, and intergovernmental organisations to develop policies and solutions to protect children from sexual exploitation and abuse online. WeProtect Global Alliance is registered as a Stichting (foundation) in the Netherlands, with a subsidiary company registered in the UK. A Global Policy Board provides expertise and advice to monitor and guide the activities of the organisation.

### Secretariat support: Praesidio Safeguarding

Praesidio is a specialist child online safety consultancy that believes that every child has a right to be safe and to thrive in the digital environment. Praesidio is committed to delivering high quality projects which help to create a better and safer online experience for children and young people.


# A Multi-Stakeholder Dialogue on Age Assurance

## Working Group on Law and Regulation

KEY TAKEAWAYS

Working Group Meetings

Virtual 10 October and 25 November 2024

# Key Takeaways
# A Multi Stakeholder Dialogue on Age Assurance

## Working Group on Law and Regulation

Virtual Meetings 10 October and 25 November 2024

The Centre for Information Policy Leadership (CIPL) and the WeProtect Global Alliance are leading an ongoing multi-stakeholder dialogue on age assurance. As part of this initiative, the Law and Regulation Working Group held two online meetings to consider the opportunities and potential challenges for age assurance created by the emerging legal landscape (with a focus on the European and UK contexts), and to contribute to a shared understanding of legal and regulatory requirements.

Attendees represented a diverse range of organisations, including child rights, privacy, safety, academia, regulators, and civil society.

The discussion took place around a fictional case study to invite input from different stakeholders with different perspectives.

The case study sought to prompt discussion of the following topics:

1. The When: Risk-based approach to age assurance
2. The What: Age assurance and complementary measures
3. The Who: Roles and responsibilities in age assurance

Below are the key points from the discussion corresponding to the three topics listed above. Each section provides the relevant part of the case study (in blue text) for context.

## Part 1: The When - Risk-Based Approach to Age Assurance

### Case Study

Peter is an 11-year-old student who enjoys spending time with his friends. He is a confident, fun-loving kid and there is always a positive atmosphere in his group. Recently Peter got a new phone which makes him feel more connected to his friends, as they have joined the same 10 educational, social media, gaming and communication services.

All of the online services that Peter uses allow users to share and access public user-generated content. At first, his feeds on these services are filled with clips about the games he plays or silly jokes that made him laugh.

One day, however, a more interesting video popped up on one of these services. Out of curiosity, Peter clicks on it expecting it to be fun.

To his surprise, the video contains violent content. Peter watches it in full, and makes him feel uncomfortable.

All of the online services that Peter uses are likely to be subject to a number of risk assessment and mitigation obligations. For example, in the EU and the UK:

- Services that are 'very large online platforms' – Arts 34-35, DSA
- Services that are 'online platforms' – high level of privacy, safety, and security - Art 28, DSA
- Services that are 'data controllers' need to have a lawful basis for processing personal data and potentially a DPIA - with many using an AADC assessment where minors are involved – Art 6, Art 35, GDPR
- User to user service – Section 3, UK OSA
- Services that are 'data controllers' need to have a lawful basis for processing personal data and potentially a DPIA – UK GDPR
- Services may also need to follow the ICO Children's Code

**Discussion Questions:**

**1. How should online services assess the risk of public user-generated content?**
**2. What mitigations should they put in place?**

## Key Takeaways from Part 1

- Age assurance should not be used solely to exclude children from inappropriate content but can also be employed to provide age-appropriate experiences that deliver tailored content. Knowing a child's age or age bracket can help ensure that children receive suitable content, supporting both children's online engagement and safer online experiences.

- Platforms face challenges in defining harmful content for children, given social, cultural, and developmental differences. There is limited guidance on age-specific harm assessments, which may lead to inconsistent evaluations across platforms. Assessing risks based on guidance from established legal frameworks, such as the "5Cs" – i.e., Content, Contact, Conduct, Contract, Context – can ensure a structured, uniform, and comprehensive evaluation.

- The use of recommender systems can raise data processing risks, especially when applied to children. Data protection authorities are increasingly focused on recommender systems especially where the recommendations are based on processing children's data. However, implementing mitigations measures, including age assurance, can reduce risks to the rights of children. In addition, recommender systems themselves can also serve as a mitigation measure for risks to children, by promoting age-appropriate content.

- Content moderation efforts via filtering, blocking and flagging can reduce the risk of exposure to inappropriate content will not always be 100% effective (as per the example in the case).

- Platforms and apps should reevaluate the types of content allowed in their terms of service. For example, where violent content is permitted, the platform may need to raise the minimum age for access and continue to improve content moderation measures to flag or filter such content for certain user groups. However, this is an iterative process that requires continued adjustment.

- Some platforms may not use age assurance because they assessed themselves as posing minimal risk to children in terms of privacy and safety. Regulators would not likely expect the use of age assurance measures for services that present minimal risk, but platform operators should nevertheless engage with regulators to ensure a common understanding of risk levels.

To conduct an appropriate risk assessment, it is important to understand a number of factors: the risk profile of a service, whether underaged users are likely to see harmful content, the type of harm, and the features of the service. Regulators such as the UK's Office of Communications (Ofcom) and Information Commissioner's Office (ICO) have issued consultations and published guidance on how platforms can determine whether a service is likely to be accessed by children. These platforms will then need to assess the risks they pose and take action to protect against such risks commensurate with the risk level. The ICO's Children's Code outlines 15 standards that online services must implement if their platforms are likely to be accessed by children. These standards are designed to guide digital services in their efforts to ensure that children's personal data is properly protected and that services meet specific safeguards for privacy and security.

## Part 2: The What - Age Assurance and Complementary Measures

### Case Study

One service Peter accesses has extensive mitigation measures to prevent young people from accessing violent content, for example:

#### Platform Design

- Service does not open to a UGC feed
- UGC on the service is only accessible for a limited duration
- Service displays warnings when accessing public UGC for the first time

#### Content Rules

- Service has clear guidelines and explainers to help users understand the rules
- Service has additional rules for public UGC requiring it to be suitable for 13+
- Public UGC cannot include violent content

#### Content Moderation and Enforcement

- Service has multiple layers of automated and human moderation
- All content is subject to automated review processes before dissemination to the public via recommendation systems
- All content is subject to human review before being widely recommended to the public via such systems
- All content is easy to report and the service responds promptly to reports

#### Monitoring

- The service sample tests the public content on its service - which shows very low prevalence of violent content
- The service monitors for underage accounts and promptly closes accounts reasonably suspected to be used by under 13s

One service has some mitigations in place but not all.

One other service has no mitigations but prohibits under 18 accounts from accessing public content. The other seven services have no mitigations at all.

**Discussion Questions**

**1. Is age assurance necessary for:**

- The platform with extensive mitigations to prevent young people from accessing violent content?
- The platform that has some mitigations but not all?
- The platform that prohibits under 18 accounts from accessing public UGC content?
- The other platforms with no mitigations?

**2. If age assurance is required, then what kind of age assurance is appropriate for the platforms in each category (low-risk, medium-risk, high-risk)?**

- Declared age?
- Highly effective age assurance?
- Multiple methods to maximise accessibility?
- Path for those who cannot successfully pass age assurance to avoid impact on user rights?
- Parental oversight/control?

**3. Does this differ in the EU vs UK?**

**4. How might this differ for adult content?**

**5. Does the kind of risk (content, conduct, data processing) shift the dial for what is required?**

## Key Takeaways from Part 2

- A key challenge for online services is determining the appropriate risk threshold for the implementation of age assurance measures. Few platforms are risk-free and even highly effective mitigation measures are unlikely to be 100% effective. This raises questions about acceptable risk levels – e.g., would one inappropriate video per 100 be an acceptable risk level, or should a stricter threshold apply (one per 1000)?

- Risk assessments should include an evaluation of the appropriateness and utility of mitigation measures, keeping in mind that certain mitigations may address safety issues but may not address other concerns, such as the lawfulness of data processing.

- From a data protection perspective, age assurance measures that process personal data must be lawful, fair, and effective to meet GDPR standards. Services employing such measures must therefore take into account the type of data they are processing and whether the processing itself could be considered high-risk. If high-risk processing is identified, the GDPR may require a Data Protection Impact Assessment to evaluate mitigations in place and ensure the protection of personal data in compliance with the Regulation (n.b. Recital 75 GDPR regarding DPIAs for children's data).

- Recommender systems can serve as a risk-minimising measure by tailoring content appropriately. These systems can help strike a balance between offering personalised experiences and maintaining safety.

- The use of age assurance measures for services that do not require users to sign-in requires further exploration and development. Allowing access without sign-in can protect user privacy, provide streamlined access, and accommodate those with technical limitations. However, the absence of a sign-in process can also introduce risks. It makes age verification and personalisation potentially more challenging with an increased risk of underage users accessing age-inappropriate content. It also makes it more difficult to track and hold individuals accountable for their actions on the platform. Parental controls to manage what children are accessing online may equally be linked to specific accounts.

## Part 3: The Who - Roles and Responsibilities in Age Assurance

### Case Study

Age assurance could be implemented at different levels for Peter:

- The operating system account Peter uses to access his device
- The app store account that Peter uses to download apps
- The 7 online services that have no mitigations for registration
- The 1 online service to support its 18+ age gate

The age assurance tool used by some services only says “yes - over 18” or “no - under 18”. As a result, these services must regularly check or reverify users' ages to ensure that their information remains accurate and up-to-date. Other services are using more robust age assurance tools and collect age data once, but the process is more complex and, in one case, Peter hit an error and has not been able to finalise the process.

Feeling frustrated, Peter:

- Minimises the services he accesses
- Finds a service on the dark web that does not use any age assurance (and also has no mitigations)

How would these solutions operate under existing European legal frameworks?

| EU | UK |
|---|---|
| DSA - provider | OSA & codes - provider |
| GDPR/guidelines - data controller | UK GDPR/AADC - data controller |
| AVMSD - provider | AVMS Regulations - provider |
| DMA - gatekeeper | DMCCA - SMS firms |

## Discussion Questions

**1. Who has primary responsibility under the different legal regimes under discussion? Are there any conflicts?**

- Can we separate responsibility for age assurance and for complementary/ alternative measures?
- What data processing considerations arise?
- What are the opportunities for interoperability in this scenario?
- How do current regulatory regimes treat interoperability versus service-level responsibility?
- What duties are owed to users? By which party? Does this change depending on the method for age assurance?

**2. What are the pros and cons of distributed approaches vs investigating a centralised, interoperable solution? And what is possible under the current regulatory framework?**

- What are the options to make distributed approaches interoperable?
- Does a centralised approach shift the burden of responsibility?
- What are the liability considerations for each approach? Where would additional regulatory guidance be useful?
- What happens with shared or sold devices?
- What effect does digital identity have on Peter's issues?
- Could a centralised approach work in a legislative environment where different services already need different age assurance?
- How can we assess proportionality/reasonableness of the options? (e.g., cost)

## Key Takeaways from Part 3

- The online ecosystem is complex, with users interacting from a variety of entry points, devices, and services.
- Many services are interconnected, potentially adding to the complexity of responsibilities among device providers, operating systems, app stores, and content providers.
- Clarity on the allocation of liability under different legal regimes is essential to ensure a shared understanding among stakeholders, a clear recognition of implementation challenges, and the effective development of policy choices leading to practical solutions.
- Collaboration among the different industry players in the online ecosystem is necessary for the development of pragmatic solutions. It should not be a binary choice between a centralised system or a distributed system. Industry should explore ways of sharing and/or distributing intelligence (such as age signals) and developing due diligence measures to ensure the holistic protection of young users where possible.
- Developing age assurance solutions can be particularly burdensome to SMEs.
- Challenges and workarounds to potential solutions—such as the increased usage of virtual private networks (VPN) to bypass location-specific measures — need to be taken into account when trying to develop effective age assurance measures.

## Who We Are

**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, 85+ 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 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.

**WeProtect Global Alliance** brings together over 300 members from governments, the private sector, civil society, and intergovernmental organisations to develop policies and solutions to protect children from sexual exploitation and abuse online. WeProtect Global Alliance is registered as a Stichting (foundation) in the Netherlands, with a subsidiary company registered in the UK. A Global Policy Board provides expertise and advice to monitor and guide the activities of the organisation.

**Secretariat support: Praesidio Safeguarding**

Praesidio is a specialist child online safety consultancy that believes that every child has a right to be safe and to thrive in the digital environment. Praesidio is committed to delivering high quality projects which help to create a better and safer online experience for children and young people.


# A Multi-Stakeholder Dialogue on Age Assurance

## Considerations Towards an Interoperable Age Assurance Framework

## KEY TAKEAWAYS

13 June 2025

# Key Takeaways
# A Multi Stakeholder Dialogue on Age Assurance

Workshop on Interoperability

13 June 2025 | Brussels

The Multi-stakeholder Dialogue on age assurance, led by the Centre for Information Policy Leadership (CIPL) and the WeProtect Global Alliance, continues its commitment towards identifying emerging best practices in age assurance that can build a common and interoperable framework through dialogues and focused workshops.

This Workshop on Interoperability provided an overview of the current landscape and future directions for age assurance. It also discussed a draft interoperability framework developed in the Multi-stakeholder Dialogue and sought feedback from stakeholders who participated in the workshop. The conversation revolved around two main parts: (i) the proposed age assurance framework and (ii) specific considerations for viable age assurance beyond 18+ verification.

Below are the key takeaways.

## Key Takeaways

As digital platforms continue to play a central role in the lives of children and young people, the need for effective, privacy-respecting age assurance continues to be a central point of discussion. Age assurance is not just a means to prevent children from accessing restricted content; it is a risk mitigation measure, often also necessitated by legal obligations. Yet the landscape for age assurance is becoming more and more complex, marked by new legal obligations, codes or guidance at increasing intervals, inconsistent technical implementations, a lack of interoperability, and limited user control.[2]

This, coupled with age limits varying across jurisdictions, creates challenges for services operating globally and burdens user experiences.

There is a growing consensus to address these challenges. A more unified, standards-based framework for age assurance is needed. Such a framework should be **interoperable across services and jurisdictions**, offer **flexibility for developers** and **minimise personal data collection** while providing trustworthy age assurance and a more uniform user experience.

CIPL and WeProtect Multi-stakeholder Dialogue on Age Assurance has explored what such a broader interoperability framework for age assurance could look like, connecting different credential holders with an application or online service.

## Main Elements of the Draft Interoperable Framework

- Digital credentials can be based on a number of sources, including governments and private issuers as well as providers of age estimation techniques offering choices and flexibility in age assurance as technology continues to evolve.

- A framework should be **technologically neutral**, aiming for broad applicability across industry applications.

- Age assurance must be **proportionate and risk-based**, meaning the level of age assurance (e.g., age verification vs. estimation) should be commensurate with the associated risk of the service or content.

- **Transparency**: Users must receive clear explanations about why age assurance is required and how it works.

- **User Autonomy**: Users should be empowered to choose whether to share assurance information with a particular relying party and which suitable credential they wish to share for verification, enhancing user agency as well as their overall experience.

- Users should have sufficient **redress mechanisms** available to challenge age assurance decisions, and control over the sharing of their age information.

- **Privacy by design** constitutes a fundamental principle of any interoperable solution. Privacy Enhancing Technology (PETs) such as Zero Knowledge Proof (ZKP) technology offer additional privacy protections, minimising data sharing and ensuring that credential holders cannot track user activity.

- **Security:** The framework should have the appropriate mechanisms in place to prevent misuse and protect from bad actors who might try to exploit the system.

- **Defines Roles and Liability Undertakings**: All the roles and the liability of each party involved in the operation of the framework should be clearly defined:

    - Age assurance providers should be responsible for the validity of signals;

    - API providers are responsible for the technical integrity of the API and supporting interoperability as feasible, and

    - App developers/website providers for implementing appropriate measures based on their risk assessments.

## Additional Considerations for an Interoperable Framework

The workshop provided an opportunity for stakeholders to engage in a meaningful discussion, gathering their insights on additional key elements to be considered for an interoperable framework.

Below some of the main takeaways:

### Ensuring fair competition, cost allocation, and clarity on liability

- Where relevant, a framework should address the commercial relationships between age assurance providers and relying parties (e.g., apps or websites) as the current practice involves direct contracts between a website or service and a verification provider.
- The framework should be inclusive and open to a multitude of solutions or signals to ensure broad utility and healthy competition, with standards that do not inadvertently exclude smaller players from participating.
- Cost allocation for the continued maintenance and functionality of a framework and the underlying technology will have to be addressed, as well as liability in case of potential negligence or errors.
- The workshop recognised a general need to move towards clear standards and accreditation of trusted signals to establish trust in the available solutions.
- An interoperable framework will be most effective if it is flexible enough to empower online platforms to comply with diverse regulatory requirements across jurisdictions.

### Cross-Sector Collaboration

- The success of an interoperability framework for sharing age signals depends on cross-sector cooperation to ensure systems are compatible, reduce friction for users, and create overall a cohesive and well-integrated experience for all stakeholders.
- A key challenge will be to identify what would constitute a trusted signal and what the accreditation process would involve. This requires active engagement of stakeholders, including:
  - those who currently provide age signals,

- those with the potential to do so (e.g. financial institutions, telecommunication providers),
- regulators who should acknowledge and define which signals can be accepted as part of an interoperable framework, and
- accreditation or verification of actors to ensure that the accepted signals meet the agreed standards.

### The role of regulators

- Regulators should foster a common understanding and taxonomy of age assurance methods. This will lead to a uniform framework that can bridge existing regulatory gaps and enable broad applicability.
- Regulators should also be open to innovative approaches, such as pilot projects and sandboxes to test a framework's effectiveness in real-world scenarios.

### The role of PETs

- Stakeholders recognised the important role of PETs to limit unnecessary data sharing. However, where an age signal is incorrect or a minor gains access to non-age-appropriate content, PETs prevent tracing the origin of the age information, which hinders online providers' ability to mitigate and ensure accuracy.
- To address this issue, a framework should consider complaint or reporting mechanisms to allow issue flagging to the signal provider in the case of conflicting age signals. For example, where a user's behaviour on a given platform indicates that they may be below (or above) the age provided through the age signal,[3] or where an age signal turns out to be inaccurate or compromised, these mechanisms would be crucial for the continuous improvement and accuracy of age assurance solutions. This should go hand in hand with overall detailed and robust appeal procedures on individual services or apps.

## Valuable Age Signals for Effective Age Assurance

Children under 18 years old engage with the digital world in diverse and complex ways, which necessitates approaches that are tailored to their developmental stages. The 13 to 18 age group presents a unique challenge: it is a broad and ambiguous range where months, not just years, can make a significant difference in cognitive maturity, and online behaviour, and move an individual from one legal threshold to the next.

Children below 13 years old often also participate in the online world; appropriate engagement will generally depend on parental supervision of this age group.

As there are a few jurisdictions in which digital IDs are issued to those below 18 years old[4], there is a need to explore more signals that can support age assurance in the 13 to 18 age range (and potentially below) to ensure that children can navigate the online world safely. These signals may indicate a user's likely age with some precision or come in the form of age bands, as appropriate. The level of access or safeguards may in some cases require granularity. Age assurance should not be an exclusionary tool but instead should be seen as a tool for risk mitigation that aims to support age-appropriate content.

### A number of sources could provide signals to be deployed in the 13+ age assurance context:

- **Mobile phone service providers** and **financial institutions** can play a constructive role by contributing to trusted age signals based on their existing customer data and relationships. Mobile phone contracts and bank accounts also often establish a direct, reliable link between a parent and child[5], potentially covering a large proportion of young users.

- **Government-held information**, such as social security, educational or health records. Of course, public bodies are often reluctant to share sensitive data, and existing GDPR purpose limitation rules restrict using data collected for one purpose (e.g., education) to be used for another (e.g., age assurance) unless the new purpose is compatible with the original.

## Age Assurance Considerations Beyond Age Signals

## Ongoing Concerns in Age Assurance

The workshop also focused on additional consideration for sustainable solutions to age assurance.

### Risk-based approach

- A risk-based approach is fundamental to effective age assurance: it is critical for tailoring protective measures to the potential risks of online services. Risk-based approach will remain central to policy discussions as technology evolves and risks shift over time.

- For example, the rapid development of AI tools creates new challenges, such as complex issues around identity verification (e.g., determining whether the user is human), that need to be carefully considered when crafting age assurance solutions.

## Parental engagement

- Parents come from different cultural and socioeconomic backgrounds and may not all have the same level of digital maturity or attitude to their children's online engagement. Many parental control tools can be complex to understand, and because they differ across platforms, using them effectively may require significant time and effort. This raises and will continue to raise questions about how to provide meaningful assistance to parents when navigating this environment.

- There should be a careful balance between the necessary levels of parental engagement and provider responsibility when it comes to developing and implementing accessible age assurance measures and parental control tools. Parents and guardians have the discretion to decide what their children should access online.

# Next Steps

CIPL and WeProtect Multi-stakeholder Dialogue is an ongoing project. Next steps include exploring further alignments on standards and protocols in the context of the interoperability framework.

For more information please contact Zeta Rizikianou (grizikianou@hunton.com) and Alison McNulty (alison@weprotectga.org).

# End Notes

[1] The UK Age Appropriate Design Code (AADC) requires online services "likely to be accessed by children" to "establish the age of child users with a level of certainty that is appropriate for the risks your data processing creates." Please see: Information Commissioner's Office (ICO), "Age Assurance – Estimating or Verifying the Age of Service Users," in Children's Code: Best Interests Framework, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/best-interests-framework/age-assurance/

[2] Below are some recent examples of new legal obligations and initiatives to develop new codes:

- In July 2025, the European Commission published the guidelines on the protection of minors under Article 28(4) of the Digital Services Act, following a consultation that gathered input from all interested stakeholders. Please see: European Commission. Commission Publishes Guidelines on the Protection of Minors. July 2025. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors
- Additionally, on the EU level eIDAS 2 Regulation is progressing. The regulation mandates EU Member States to provide EU Digital Identity Wallets.
- The OAIC is developing a Children's Online Privacy Code, expected to be finalised in 2026, and launched a consultation to gather feedback from industry, children, parents, civil society, academia, and other stakeholders. Please see: Office of the Australian Information Commissioner (OAIC), Children's Online Privacy Code: Consultation for Industry, Civil Society, Academia and Other Interested Stakeholders, https://www.oaic.gov.au/engage-with-us/consultations/childrens-online-privacy-code-consultation-for-industry,-civil-society,-academia-and-other-interested-stakeholders
- The Office of the Privacy Commissioner of Canada (OPC) launched a consultation to inform the creation of a federal Children's Privacy Code clarifying obligations under PIPEDA, and is seeking input from industry, parents and guardians, child-rights groups, educators, and youth to ensure its provisions reflect practical challenges and protect children's interests. Please see: Office of the Privacy Commissioner of Canada, *Exploratory Consultation on a Children's Privacy Code*, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-children-code/expl_children-code/
- From 25 July 2025, platforms must use effective age assurance mechanisms to block children from harmful content, including pornography, self-harm, suicide, eating disorders, bullying, hate speech, dangerous stunts, or ingesting harmful substances. They must also offer clear reporting tools for parents and children. Please see: *Online Safety Act*, collection page, GOV.UK (Department for Science, Innovation and Technology), published 24 July 2025, https://www.gov.uk/government/collections/online-safety-act
- On October 2024, France's regulator ARCOM published a binding age verification standard for pornographic sites, mandating robust, privacy-preserving measures such as double anonymity, with full compliance required by 11 April 2025. Please see: Osborne Clarke. (2025, January 9). *French regulator Arcom's standard for online age verification rolls out in 2025*. https://www.osborneclarke.com/insights/french-regulator-arcoms-standard-online-age-verification-rolls-out-2025
- Spain released technical specifications for an age verification system using W3C Verifiable Credentials to ensure GDPR-compliant, privacy-preserving proof of age for accessing adult content. Please see: Ministerio para la Transformación Digital y de la Función Pública. *Especificaciones técnicas*. https://digital.gob.es/especificaciones_tecnicas.html
- Greece launched the Kids Wallet app as part of its National Strategy for the Protection of Minors, enabling parents to manage children's digital access through parental controls linked to official digital identity systems. Please see: Ministry of Digital Governance. (2025). *Protecting minors from internet addiction: National strategy*. Hellenic Republic. https://mindigital.gr/wp-content/uploads/2025/03/%CE%9DStrategy_ProtectM_long_ENG.pdf

[3] For example, providing a "contra indicator" or "red flag" based on community moderators or peer reporting.

[4] In Denmark, from the age of 13, individuals in Denmark can obtain MitID, the national digital ID, which allows access to certain self-service platforms such as online banking or tax services—though some services remain restricted until the age of 15.Please see: MitID, "13 to 14 Years Old," *MitID Help Universe*, https://www.mitid.dk/en-gb/help/help-universe/13-to-14-years-old/.
In India, there is no age limit for obtaining the Adhaar Card (a unique identification document issued by the Government of India); individuals of any age, even newborns can enrol for one. This system is beneficial as it helps in availing various government services and schemes from an early stage. Please see: "Aadhaar Card Age Limit," *Bajaj Finserv*, https://www.bajajfinserv.in/aadhaar-card-age-limit

[5] This is because children cannot open an account or enter into a contract without parental consent. The age limit varies across jurisdictions.

## Who We Are

**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, 85+ 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 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.

**WeProtect Global Alliance** brings together over 300 members from governments, the private sector, civil society, and intergovernmental organisations to develop policies and solutions to protect children from sexual exploitation and abuse online. WeProtect Global Alliance is registered as a Stichting (foundation) in the Netherlands, with a subsidiary company registered in the UK. A Global Policy Board provides expertise and advice to monitor and guide the activities of the organisation.

Centre for Information Policy Leadership (CIPL) & WeProtect Global Alliance

# A Multistakeholder Dialogue on Age Assurance

*Proposal for a Wallet/ Credential Manager Framework*
*for Age Assurance Solutions*

**Introduction**

The digital world, while offering unparalleled opportunities for education, connection, and creativity, also presents challenges in safeguarding children and young people from age-inappropriate experiences. The current landscape of online age assurance remains fragmented, characterised by inconsistent technical implementations and a lack of unified standards. This not only burdens app developers and other service providers but, crucially, leads to a disjointed and often frustrating experience for users themselves - including for parents.

Recognising this critical need, we commend the European Commission's proactive steps in addressing online safety for minors, particularly through initiatives under the Digital Services Act (DSA) and the ongoing development of an EU-wide age verification framework. In this context, we are pleased to note that the recently released Commission guidelines under Article 28 of the DSA align well with the vision of a robust and privacy-preserving age assurance framework CIPL is working to develop. The Commission's commitment to fostering a safer internet for kids (BIK+ Strategy) and exploring privacy-preserving solutions, such as the age verification app leveraging zero knowledge proof (ZKP) technologies and the upcoming European Digital Identity (EUDI) Wallet, is a vital step forward. Similarly, in the UK Ofcom has issued extensive guidance on effective age assurance for different service levels in scope of the UK Online Safety Act and lists a variety of age assurance methods that can be considered highly effective. It also highlights the importance of interoperability between the possible age assurance methods, to ensure a more streamlined experience for the user and ultimately limit the collection of personal data.

We agree that further potential for protecting minors and streamlining compliance lies in enabling further choice for developers to leverage some of the recent advancements made by technology platforms. The introduction of credential management APIs - which empower users to share identity signals from their preferred stored credential with relying parties - by companies like Google[1] and Apple[2] represents a pivotal moment. These APIs offer the promise of standardised, privacy-preserving mechanisms for age

[1] Google. 2024. Credential Manager API. Android Developers. https://android-developers.googleblog.com/2024/12/build-high-quality-enagaing-age-appropriate-apps.html
[2] Apple. 2024. Declared Age Range API. Apple Developer Documentation. https://developer.apple.com/support/downloads/Helping-Protect-Kids-Online-2025.pdf

assurance that could be used by app developers and website providers to offer flexible age-appropriate experiences to their users.

However, the efficacy of these promising developments hinges on the development of a broader, interoperable framework. By defining shared principles, technical standards, and levels of assurance, these powerful APIs can operate seamlessly across diverse platforms, providers, and jurisdictions. This would deliver significant benefits for all stakeholders:

- for all users, a consistent, less intrusive, and highly secure experience when verifying their age online;
- for minors, a more age-appropriate experience across the mobile ecosystem;
- for developers, drastically reduced complexity and uncertainty by providing clear guidelines and alleviating the burden of navigating disparate regulatory requirements.

For this to occur, industry needs key regulators in both the privacy and content spheres to encourage these developments by aligning on practical, flexible guidance that:

- holds companies who know their services' risks best ultimately responsible for implementing age assurance that is proportionate to those risks;
- 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;
- balances the need to protect user privacy with the need to provide robust age signals to support age appropriate experiences;
- incentivises cross-industry standards through recognition of developing and other standards that promote consistency; and
- spurs adoption and integration of official digital credentials and related apps by supporting integration with developing industry approaches to expand usage and promote interoperable methods that support the entire ecosystem.

This discussion document provides a draft framework to support an interoperable approach to age assurance. It outlines principles and elements for consideration as a part of an infrastructure approach, while acknowledging that developers may choose alternative and/or complementary approaches to meet their age assurance objectives or regulatory obligations. Digital credentials infrastructure could be a powerful option for interoperability and user convenience but should not be considered a mandatory single point of entry.

## 1. Framework Objectives

The proposed Interoperability Framework for Age Assurance Solutions seeks to:

- Leverage a **common taxonomy** and classification of age assurance methods: This aims to create a shared understanding and common language for all stakeholders. It involves defining and classifying different methods based on their confidence levels (Levels of Assurance - LoA) and the associated privacy impacts (e.g., anonymous, pseudonymised, identifiable). An example is the latest ISO standard draft.

- Promote the need for **technical standardisation** for signal generation, exchange, and verification: There is a need to develop and promote robust, privacy-preserving technical standards for how age signals are generated, exchanged and verified. This includes emphasising data minimisation principles and exploring advanced Privacy-Enhancing Technologies (PETs), like ZKP technologies[3], ensuring seamless and secure data flow while protecting user privacy. For example, through the ongoing efforts to finalise an ISO framework on age assurance.
- Support **trust and accountability** among ecosystem actors (governments, regulators, providers, platforms, users): Beyond technical specifications, building confidence in the system is paramount. We believe a crucial consideration is comprehensive user education. As this introduces a fundamentally new digital experience for users interacting with apps and websites, a robust educational component will be essential to successfully introduce and embed this new approach for both child and adult users. Thus, this objective focuses on establishing mechanisms for transparency, ensuring users understand how their age is verified and what data is used and stored through, among other things, where common user interfaces could be used to help develop user comfort with verification. Supporting relying parties like developers in understanding the source and reliability of relevant signals is also paramount and part of this effort.
- Create pathways for **cross-jurisdictional recognition** and mutual compatibility: This includes exploring mechanisms for mutual compatibility and recognition, leveraging existing EU initiatives like the European Digital Identity (EUDI) Wallet for recognised age credentials. Such pathways are crucial for reducing duplication of effort and ensuring a consistent user experience across the single market and beyond.

## 2. Foundational Principles

### 2.1. Risk-Based Proportionality

[3] Zero-knowledge proof is a technique that enables one party (the prover) to prove a claim to another party (the verifier) without revealing anything more than the truth of the claim. Through the use of complex mathematical algorithms, the proof is generated in such a way that it is computationally infeasible for someone who does not know the claim to generate a similar or related proof.
A zero-knowledge proof has three main properties:

- Completeness: If the claim being proved is true, then an honest verifier will be convinced of this fact with high probability.
- Soundness: If the prover does not know the claim, then he cannot deceive the verifier with high probability.
- Zero-knowledge: The verifier does not learn anything other than the validity of the claim. There are two main types of zero-knowledge proofs: interactive and non-interactive.

Centre for Information Policy Leadership (2023) *Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age*.
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf

A key principle underpinning an effective and proportionate age assurance framework is the adoption of a risk-based approach. This means that the stringency and invasiveness of the age assurance method applied should be commensurate with the potential harm that age-inappropriate content or experiences could pose to a minor. Instead of a "one-size-fits-all" solution, a risk-based approach allows for flexibility, ensuring that less intrusive methods are used for lower-risk scenarios, while more robust verification is reserved for higher-risk contexts.

While first-party mechanisms, such as machine learning-based age estimation models, can be suitable for certain contexts, access to some high-risk 18+ goods and services may require a higher degree of confidence in age verification (e.g., adult content, gambling).

Risk levels should be aligned with service-specific risk assessments, where available, drawing on approaches such as **Ofcom's risk-based model** under the UK Online Safety Act or the Commission's similar approach with regard to minor risks in the proposed Guidelines for Article 28 of the DSA. More broadly, companies should understand the risks posed by their services where those are likely to be accessed by children and be expected to apply the level of assurance best suited to address those risks.

### 2.2. Privacy by Design

In line with the foundational principles of data protection and privacy, particularly those enshrined in the GDPR, any age assurance framework must be designed and implemented with a paramount focus on safeguarding personal data. This commitment necessitates a proactive and integrated approach that prioritises several key areas:

Age assurance must be implemented in accordance with data protection and privacy principles, prioritising:

- **Data minimisation**: The system must be engineered to collect and process only the minimum amount of personal data necessary to confirm age. The aim is to achieve the desired level of assurance with the least possible data footprint and providing the minimum needed signal. Ideally, data protection authorities will align on support of a range of appropriate signals.
- **Anonymisation or pseudonymisation**: Rather than linking age directly to a user's real-world identity, interoperable age assurance mechanisms should strive to operate with data that has been obfuscated in a manner that mitigates risks of reidentification. This reduces the risk associated with data breaches and enhances user privacy by default.

**PETs** can support robust age assurance while maintaining privacy. For example:

- Zero-knowledge proofs: ZKP technology allows users to prove they meet a certain age requirement without revealing unnecessary personal details.
- Selective disclosure credentials: Building upon verifiable credentials, this would allow users to selectively disclose only the specific attributes required for age verification (e.g., "over 18") from a broader digital identity credential, rather than revealing their full identity document.
- Cryptographic age attestations: These involve trusted third parties issuing signed attestations of a user's age, which can then be presented to service providers without the need for the service provider to directly interact with the identity provider or store sensitive age data.

### 2.3. Transparency and User Autonomy

User empowerment and transparency are cornerstones of a trustworthy age assurance framework. All users, regardless of their technical proficiency, should receive clear, accessible, and concise information about:

- The nature of an age check: This includes explaining *why* an age check is required for a particular service or experience.
- Available redress mechanisms: Users should be able to obtain their age information and be provided the ability to request an update if they believe it is incorrect.
- Users should be empowered with a level of control over their age information and should be asked to consent to the sharing of their information.
- Where necessary, parents or guardians should have that same level of control over the sharing of the age information of the supervised child.

## 3. Interoperability Standards for Digital Credential Holders

### 3.1. Platform Neutrality

Digital credential holders, including for example digital wallet providers (private or government backed digital wallets) or digital age verification apps, can allow users to store assurances for their age (e.g., verified credentials from a trusted issuer) in their digital wallets or similar credential holder. Digital credential holders can leverage trusted credentials from first or third parties, or tools available through the digital wallet, including verification by government or other official IDs.

Digital credential holders should allow users to share assured age signals from trusted credentials in their digital wallets. For example, users should be able to share assured age signals with:

- app stores to download age gated app;
- app developers when registering for an account on an age gated service;
- app developers to access age gated features;
- web browser apps when seeking to access an age gated website.

Digital credential holders should work with industry to consider whether and how to support the integration of other forms of age assurance into the digital wallet model, including estimation (such as facial recognition) and inference technologies (such as models analysing user behavior).

Where credential APIs are provided by an operating system or elsewhere in the software stack, these should support sharing age-related information between users and developers through digital wallets or other digital credential holders.

### 3.2. Standards

The framework needs to be flexible enough to accommodate diverse regulatory landscape, including technical specifications from multiple regulators operating in different regulatory contexts, for example:

- Security standards are a key consideration, particularly when thinking beyond government-issued IDs and credentialed solutions. This could be handled through the developing ISO standard or a similarly respected body.

## 4. Roles and Responsibilities

### 4.1. Age Assurance Providers

In an infrastructure built on trust and verifiable credentials, allocation of responsibility is paramount. Therefore, a fundamental principle of this framework is that the original issuer of the credential bears responsibility for the accuracy and validity of the age signal it provides related to that credential, as appropriate based on the facts and circumstances.

This means that the entity which initially verifies a user's age (e.g., a government body issuing a digital ID, a bank performing KYC, or an accredited third-party age verification service) and subsequently issues a verifiable age credential or attestation, is accountable for the correctness of that information at the point of issuance, taking into account the agreed-upon level of assurance of the credential and having exercised reasonable care.

### 4.2. Credential Holders

While the issuer holds responsibility for the accuracy of the age credential itself, it is equally crucial to define the scope of accountability for other actors within the age assurance ecosystem, particularly digital wallet providers or other parties providing the infrastructure to facilitate the sharing of age information.

### 4.3. API Providers

Credential APIs are foundational infrastructure. Providers of this technology are primarily responsible for ensuring the technical integrity and functionality of the mechanisms that enable the user to present their age credential to a relying party and are neither processors nor controllers. Ensuring these providers are appropriately positioned with liability protections, for example regarding the accuracy of the age signal they convey, will help spur continued innovation.

### 4.4. App Developers and Website Providers

The framework must empower app developers and website providers with the flexibility to specify their precise needs regarding age assurance, aligned with their service's risk profile and regulatory obligations, where they chose to rely on a third-party signal via this framework. This means:

- App developers and website providers should be able to specify the *level of assured age signal* they require from a digital credential holder, based on available signal and the assessment of their compliance needs. This could range from a simple confirmation of being above a certain age threshold (e.g., "over 18") to a precise date of birth, depending on their specific requirements. Users should have the choice whether to share after receiving sufficient notice.

- The app developer and website provider are solely responsible and liable for decisions when and how to use that assured age signal, including whether it needs that age signal, depending on the risks associated with their service, user choice, and regulatory guidance.