Age Verification Providers Association

Helen Dixon
Commissioner for Data Protection
Data Protection Commission
Children's Policy Unit
21 Fitzwilliam Square South
D02 RD28
Ireland

By email: childrensconsultation@dataprotection.ie.

31st March 2021

Dear Ms Dixon,

Consultation response: Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing

Thank you for the opportunity to comment on this excellent guidance.

The Age Verification Providers Association is the global trade body for the providers of privacy-protecting, standards-based age assurance technology.

We welcome this document and in particular its consistency with the UK ICO's Age Appropriate Design Code. The worldwide web is a global entity so consistent regulation is not only economically desirable but also a practical necessity.

Effective online age-gating is already in operation.

In your introduction you point out that '*jurisdictions all over the world have struggled with effective means by which age-gating could be implemented on the Internet*'. We would contend that effective means do already exist and are, indeed, fully operational when it comes to the sale of age restricted goods and access to services such as gambling. Thousands of checks are made every day.

With better access to government databases, these systems could easily be extended to allow children to prove their age anonymously online. While this technology was originally designed to protect the privacy of adult users, it is surely even more important that we enable children to safely navigate the Internet and gain access to old age-appropriate content, in line with their rights, without demanding that they expose their identity to every website they visit.

We would be pleased to engage with you and stakeholders across all sectors designing codes of conduct under section 32 of the 2018 Act to explain the capabilities of the latest technology for age assurance (a term which covers both age verification and age estimation techniques).

We agree with your view that organisations should comply with the standards and expectations when the services provided are directed at, intended for or likely to be

accessed by children. Your emphasis that "likely to be accessed by a child" means that this is more likely than not is also critical. There is plenty of evidence, for example, that pornographic websites, which harvest and process personal data such as IP addresses as a critical component of their commercial business model[1], are extensively accessed by children, even though they may even state they are not *intended* for children.

Legal backdrop

It is logically impossible to apply the rights conferred on children by international and domestic law in the context of the internet, if they are not identified as children in the first place. Age assurance is, therefore, not an objective in its own right, but the basic foundation for the delivery of any rights or policies related to age.

Verifying parental consent

As providers of age verification technology, we are also addressing the need for verifying parental consent as an essential extension of our services. Validating parental consent requires addressing two separate points:

1. Is consent given?
2. Was that consent given by the holder of parental responsibility over the child?

We agree that this should be a dynamic issue which is kept under constant review in light of emerging technologies and which is subject to regular efficacy assessment. The best way to achieve this is to require compliance with relevant standards which can adapt more easily than legislation and regulation. BSI PAS 1296:2018 currently identifies best practice for age-checking. It is being upgraded to an ISO standard. Meanwhile, an ETSI standard for obtaining parental consent is also in development for the European Commission through a pilot project it is funding to deliver European infrastructure for age verification and parental consent. Subject to the signature of the grant agreement, we are a member of the consortium appointed to deliver this over the next 18 months, and would welcome the close involvement of your Office in this project (see www.euCONSENT.eu).

These international standards can define levels of accuracy against which existing and emerging methods may be measured, allowing new methods to be added to the range of options available simply through the audit and certification process.

The rapid development of technology in this area, and a fiercely competitive open market in the provision of AV and parental consent services, means that the use of these techniques need not be expected only of 'technology and internet companies' but can reasonably be required of all sites which carry content which is potentially harmful to children. We should not be under-ambitious when it comes to child protection.

What constitutes a 'reasonable effort' is moving rapidly as the technology and the level of adoption progresses. It will, within 2-3 years or less, be rare to find an adult internet user in the EU who has not undergone some form of age verification for a purchase, service or content, and with the interoperable infrastructure being developed by the EU, this will be available through other age assurance suppliers to any of their clients. With such checks typically costing cents rather than euros to perform, and in many cases, only required by regulators when an account is first opened or on the first visit to a website, there will soon

[1] Tracking sex: The implications of widespread sexual data leakage and tracking on porn websites E Maris et al https://arxiv.org/pdf/1907.06520.pdf

be very little friction or cost to all sites establishing the age-range of their users to the level of assurance appropriate for their content.

Age verification mechanisms

We agree that "the technological area of age verification mechanisms and tools is still very much in development" but this phrasing may inaccurately imply they are not already very well-developed, and operating on a daily basis very effectively.

Fundamentally, the specific technical method is less important than the overall effectiveness in terms of accuracy and reliability that a particular method can offer. For this reason, given the speed of technical development in the area, we again recommend that regulators refer to the latest international standards to set the benchmark for 'reasonable efforts' when it comes to age assurance.

We apologise for not contributing to your 2019 consultation which pre-dated our capacity to respond internationally, but would like now to provide the input you sought on appropriate methods for age verification.

- The highest level of assurance can currently be achieved through electronic Identity Document Validation Technologies (e-IDVT) where the data in official documents, such as passports, national ID cards or driving licences, are checked using the near field communications (NFC) chip embedded within them against the individual claiming them as evidence of age. The system may include an initial and periodic 'liveness checks' where the user must record a new image or video which is compared against elements of the biometric facial data from the chip stored securely with the age verification token.
- Checks can also be achieved without reading the NFC chip and instead validating the machine-readable zone on such documents where the date of birth is encoded along with other security features to prevent alterations.
- For users who prefer not to use such documentation or do not have access to it, age checks can be completed by reference to third party databases such as credit reference agencies or the electoral roll. These offer a lower level of assurance given the lack of any photographic check but, for many situations, regulators deem this to be sufficient.
- This is similar to the use of payment services only available to adults, or checks made through the open banking system, or confirmation from mobile phone networks that their customer has already proven themselves to be an adult.
- If users do not wish to divulge any of the above evidence, then there is also the opportunity to use age estimation techniques. By far most advanced of these is facial analysis. This can now discern the age of a user from a picture within less than +/- 2 years with a degree of accuracy that far exceeds the ability of a human being to estimate age and indeed delivers correct results (within this margin) that exceed 99.9%. So, again, for many use cases, this is more than sufficient and only fails at the margins where a user is estimated to be within two years of the age restriction and further evidence is required if there is an exact age required by law.

Estimation techniques are continuing to evolve with theoretical and practical steps towards the use of natural language processing, voiceprint analysis, touch screen gestures and any

other behaviours which evolve in line with age to train artificial intelligence through machine learning to estimate the age of a user.

And while this is not possible for new users, platforms which already hold historic data from users can, with the appropriate permission, analyse that data to estimate age. The accuracy of this process will depend on the nature and quantity of data available, so should be subject to the same assessment against international standards before being accepted a fit-for-purpose in protecting children from particular levels of potential harm. We would argue this is best done independently but certified providers, rather than by platforms with a vested interest, and whose already considerable market dominance would only be augmented if they become the de facto gatekeepers to an age-assured audience.

Finally, there is a risk of confusion when it comes to using parental attestation, either in its own right or through existing parental controls which have been established as a proxy for age assurance. Pragmatically this may be better than nothing but it is critical to remember that much of the legislation which requires forms of age assurance it was developed because policy makers we're not confident that parents had the knowledge ability or motivation to manage childrens' use of the Internet. This could be either by failing to prevent access to unsuitable material or by refusing to allow it if they wish to block access to certain content e.g. LGBTQ+. In each case, independent age assurance will better protect the rights of children as a whole.

More than just box-ticking

Most regulators rightly exclude self-declaration as a legitimate means of age assurance. However, it can be used in combination with any of the above techniques to provide a layered approach to improving the level of assurance about a user's age.

International standards also assist in defining the degree of confidence offered by combinations of age assurance techniques, and give the opportunity for independent validation and certification of any given method or combination of methods to deliver a particular level of accuracy and reliability.

Access to data

A significant limitation on age verification for children is the lack of access to reliable age data which is normally held only by official government bodies. This is usually because of quite reasonable caution against the abuse of children data. This dilemma is being addressed through a pilot in the UK which allows for "one-way blind checks" of HM Passport Office data to confirm that the details provided by a user to an age verification provider all the same as those held by government. The provider does not see the data itself but is merely informed as to whether the details supplied are completely correct or inaccurate in some undefined way. Were this technique to be extended to pupil records, for example, it would revolutionise the ability of AV sector to provide accurate age assurance. Clearly such access needs to be limited to tightly regulated and audited organisations to prevent abuse but this would be a very simple reform, delivering a step-change in the effectiveness and accessibility of age verification. This would require action by governments in every Member State of course.

We trust this response is helpful. Do not hesitate to get in touch if you have any further questions or we can provide advice in any way.

Yours sincerely,

[redacted]

[redacted]

About the AVPA

Our current membership includes AgeChecked, AGE-ify, Digital Identity Net, Experian, GBG, Pay360, VerifiiD, VerifyMyAge, Verime, W2 and Yoti.

As an association, we work to:

- Inform and educate the public, industry, and media, on age verification solutions and technology.
- Promote a positive image of effective age verification and the age verification industry.
- Represent the industry to regulators and law makers for the advancement of best practice, socially-responsible age verification policy.

The AVPA was formed in 2018 from organisations involved in the UK's Digital Policy Alliance age verification working group, and created and in response to a need for a uniform voice for of the industry.

The AVPA is governed by a representative Board drawn from its member organisations.