Age Verification Providers Association
557B Wandsworth Road, London, SW8 3JD
+44 (0) 7811 409769 | iain@avpassociation.com

To: DG CNECT – CNECT F2

Digital Services Act – guidelines to enforce the protection of minors online

We are a global trade association representing 30 providers of online age verification and age estimation technology solutions, collectively termed age assurance by the ISO's Committee Draft standard, 27566. We are providing input and evidence on age assurance and verification processes, including standards, technologies and organisational design of an ecosystem to deliver these essential protective measures for children online in an effective and efficient manner.

While the Digital Services Act does not include any explicit requirement for digital services to implement age assurance, it is a foundational requirement if providers of online platforms are to put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, unless adequate measures are put in place for users of all ages.

Leading platforms have begun to apply age assurance already

Many online platforms accessible to minors are already adopting a wide range of methods of age assurance, selected to apply a proportionate approach to prevent harm to children. At this point in time, the most common approach is for the platform to conduct basic surveillance of its existing users, looking for anomalies that create 'red flags' that a self-declared age may be inaccurate, then redirecting the user to a specialist third-party age assurance provider to conduct more rigorous age checks. While this approach has not been implemented for long, so it is hard to evaluate its effectiveness at an early stage, it has been adopted by some of the world's largest platforms and has the potentially to deliver a quick win using existing technologies if this model is replicated across the other major digital services.

There are a number of options for how the approach to age assurance in the EU may develop beyond this in the short, medium and long term which merit consideration.

The EU Digital Identity Wallet was not designed for the age assurance use case

The target date for each Member State offering an EU digital identity wallet to its adult population is 2026, but it will take some time after that point before the majority of EU citizens have decided to take advantage of this opportunity. In the meantime, there are pressing demands for age assurance already in existence today – these arise from GDPR, the Audio-Visual Media Services Directive and the DSA, as well as specific legislation relating to certain goods sold online and services accessed on the Internet. Enforcement processes have already been initiated by the Commission for certain Very Large Online Platforms, so simply waiting for the Wallet is not an answer in the short or medium term, until there is widescale adoption. Even in the longer term, alternative methods will be necessary to avoid excluding citizens without wallets and non-EU citizens passing through the continent. And there are currently no published plans to give wallets to minors in every Member State, so this is not going to help platforms enforce minimum ages defined in their terms and conditions, or the "digital age of consent" in Article 8 of GDPR which ranges from ages 13-16.

Another critical consideration is whether using the EUDI wallet meets the requirement for anonymity that is associated with certain sensitive age verification use-cases. The French and Spanish regulators have both

sought to extend the requirements for age assurance solutions to guarantee a "double-blind" protection whereby it is technically impossible for the user to be identified by the digital service they are accessing, and for the user's online activity to be tracked as a result of an age assurance solution.

The current requirements for the EUDI wallet being transposed from the Architecture and Reference Framework (ARF) to the Implementing Act were explicitly not originally designed to deliver this "double-blind" age verification use case. With any technology, it is a significant risk to assume that a solution delivers to requirements for which it was not originally designed.

From our discussions with those involved in developing the ARF, there is a question as to whether it will inherently meet this requirement as it is being built today. A 13+ and 18+ standalone attribute has been proposed (which is a little confusing given the wallets are only to be issued to adults in most Member States, and we know there are legal requirements applying at 14, 15 and 16 as well), but the wallet is fundamentally an identity solution, and its processes all start with identification at a high level of security – giving rise to concerns that without some design adjustments, it will not be fully anonymised. A new largescale pilot currently being procured by the Commission will explore this question, but we expect it to conclude that changes are required to the specification of the wallet to ensure it meets data protection regulators' exacting new standards for both un-traceability and un-trackability.

We recommend that Commission should take a cautious approach, and perhaps only assume that the EUDI wallet can solve the age verification use case in the longer term, only for 18+, and with some modifications which would need to be rolled out across all wallets in each Member State once they have been developed and approved.

Effective, privacy-preserving age assurance solutions already exist today

The good news is that there are already widely-used, effective, privacy-preserving age assurance solutions available, and they work for both adults and children. The age assurance sector has developed rapidly over the past decade, establishing independent third-parties who confirm users' ages, then anonymously respond to inquiries from platforms about the age qualification of users. These may be conventional verifications based on identity documents or authoritative data sources (banks, credit agencies, electoral roll) or increasingly accurate innovative age estimation tools, based on facial images, voiceprints, email usage or even hand movements.

Over a billion such age checks have taken place, regulated under GDPR to guarantee privacy-by-design and data minimisation. The platforms which commission these services exercise due diligence to protect their customers from data breaches, which can have devastating consequences for their customer base and reputation. The Age Check Certification Scheme is an accredited standard against which suppliers can be audited and certified to give both platforms and users confidence in the age assurance solutions being adopted.

So rather than assuming there is a need for a novel interim solution, the Commission should perhaps first pause to consider the extensive range of effective age assurance mechanisms already available, and widely used without any data protection incidents today.

The French CNIL Double blind approach

We understand that an option being considered is to design a new interim solution based on the theoretical model developed for a 'double-blind' solution by the French data protection authority, CNIL. Frankly, we believe this is a solution in search of a problem. There is no evidence of any, let alone widespread, data

breaches from current widely-deployed age assurance processes. Existing regulation – in particular data protection requirements under GDPR - already protect the anonymity of users.

This is already a low-risk technology because there is generally no need, and therefore no legal justification, to retain any personal data after an age has been checked. The simple structural protection of using a third-party age assurance provider is sufficient to provide protection, unless the Commission lacks confidence in the implementation and enforcement of GDPR. If it has no confidence in this legal framework's ability to protect users' privacy, why would suppliers' claims to be adhering to the principles of a more complex cryptographic solution be any more credible? The existing mechanisms for third party age assurance already provide adequate protection for users and have a strong track record. If a bad actor were to undermine the current system, they could as easily undermine any future cryptographic approach. In each case, we are reliant on suppliers behaving how they claim they will, and if they do, then user data is safe in both cases.

The CNIL solution may be academically perceived to be attractive but there are some significant questions about how it can work in practice. From our discussions with Arcom and CNIL, we learnt:

(1) There is no intention to define a standard to which suppliers of age attributes must operate. Without this, how will online platforms know they can rely on the ages recorded on anonymous digital certificates? Conformity Assessment Bodies would need to audit and certify all issuers to give platforms confidence in the age information they rely upon, given they cannot know themselves which organisation generated the certificate.
(2) There is no plan to establish a certification authority that would control the public key infrastructure which is needed to manage the use of digital age certificates, ensuring platforms can authenticate certificates from multiple issuers.
(3) The regulators could not explain how they saw the business model operating to sustain a market in the supply of age certificates – if the issuer does not know which platform is using their certificate to check age, then the issuer cannot invoice that platform for this service.

In its first iteration, we understood its intention but could not see how it would be implemented without this additional infrastructure and governance, and how a commercial model could fund its operations.

We know that providers in France have built upon the original concept to deliver solutions they claim will achieve this double-blind outcome, but we struggle to see how this is feasible without (1) a standard (2) auditors (3) certification and (4) some creative mechanism to enable a sustainable commercial model.

We are also concerned that, as with any largescale technical project, this will take longer to deliver successfully than intended. If the ambition for this temporary solution is only to address the 18+ use case, then it is likely that a solution based on the wallet, for which a largescale pilot is already being procured by the Commission, will be ready just as quickly.

We recommend the Commission considers more carefully the use of existing tried and tested age assurance solutions. It could increase the surveillance of providers for their data protection measures. It could require them to be independently certified following audits by conformity assessment bodies. It could even establish a licensing arrangement with only certified age assurance providers being permitted to offer the service after rigorous data protection and security audits based on international standards.

The alternative approach of developing an entirely new interim solution built on an academic model which gives rise to some fundamental design questions would be sub-optimal. The purpose of an interim solution

Age Verification Providers Association
557B Wandsworth Road, London, SW8 3JD
+44 (0) 7811 409769 | iain@avpassociation.com

is to solve the challenge of age assurance as quickly as possible – this is far better achieved by building on what exists and works today, than embarking on a fresh project.

Spain's age verification app

The Spanish AEPD option was more straightforward. They propose to create an age verification app on any device accessing the Internet, which would check the user's age from their EUDI Wallet, and then allow apps and browsers on the device to create age-appropriate content and functionality. This solution is constrained by the adoption of the wallet by EU citizens, and only works for adults so is not helpful for GDPR, age-appropriate design or minimum ages for social media. As with the CNIL plan, it also lacks any obvious commercially sustainable business model, so would need to be supplied, maintained and serviced by Member States. The customer service demands alone should not be underestimated, and then all the platforms, sites and apps need to be re-designed to integrate with the AV App, and to apply differential policies based on the age range reported.

Building on what works today

The Age Assurance industry has noted all these innovations and the concerns behind them carefully, and working through euCONSENT ASBL, the non-profit organisation established in Belgium to which all the intellectual property from an EU-funded project of the same name was donated, has created a new hybrid solution, that we believe meets all the requirements of EU laws, and the stipulations of data protection authorities. This is the AgeAware ecosystem, and euCONSENT is currently consulting on a detailed specification document. https://euconsent.eu/feedback-on-ageaware-specification/. A proof of concept is being built by the end of 2024 and it has widespread support from across the age assurance sector.

In summary, it is a tokenized solution where users (of all ages, not only adults) can agree to hold a digital token on their device (laptop, smartphone, tablet etc.) that indicates they have completed an age assurance process to a specified level of age assurance. Subsequently, other digital services – both apps and websites – can see those tokens and choose to use them to check the user meets an age condition rather than requiring a fresh age check. Tokens can be created through both age estimation and age verification methods – the method will influence the level of age assurance of the token. The lifespan of the token is limited, with higher levels of assurance generally shortening the validity period of the token – so this solution remains focused on proving the age of a user, not labelling a device which might be shared with or passed on to younger users. Re-authentication can be triggered to confirm the user is still the same person to whom the token was issued. A tallying service reports the number of times each digital service uses tokens issued by each age assurance provider, enabling a sustainable commercial model without breaching anonymity.

We would be pleased to facilitate further engagement between the age assurance industry and the Commission to explore these options, and create a pragmatic roadmap that delivers protection for children as quickly as possible, building on what is already working effectively today, and taking an evolutionary approach, rather than risking being dependent on a brand new development of an interim solution with no track record.

Yours faithfully,

Iain Corby
Executive Director