22 May 2026

CHILDREN'S ONLINE SAFETY AND AGE VERIFICATION CONSULTATION PAPER RESPONSE

1. INTRODUCTION

1.1 Spilsbury Holdings Limited t/a Aztec Labs ("**Aztec Labs**") welcomes the opportunity to respond to the "*Growing Up in the Online World: A National Conversation*" consultation issued by the Department for Science, Innovation and Technology, presented to Parliament by the Secretary of State for Science, Innovation and Technology, dated March 2026 (the "**Consultation**").[1]

1.2 Aztec Labs is a UK-headquartered software development company building open-source, blockchain-based software with a focus on zero-knowledge proofs ("**ZKP**"), a form of advanced cryptography discussed in detail in this response. Aztec Labs has recently acquired and is developing ZKPassport ("**ZKPassport**"), an open-source, permissionless, and self-custodial digital identity system (available on iOS and Android) that uses the same International Civil Aviation Organization ("**ICAO**") open standards relied on globally in airports and border systems to authenticate electronic identity documents. ZKPassport enables individuals to prove specific facts about themselves (such as nationality, age, or document validity) directly from their government-issued electronic passport, national e-ID card, or electronic residence permit, without revealing any other personal information. The technology has been battle-tested in production, performing approximately 30,000 document checks and ZKP proofs.

1.3 At its core, age verification is a digital identity problem. Every time a user proves they are over 13, 16, or 18 to access an online service, they are making an identity assertion. The critical question for this Consultation is whether that assertion requires individuals - including children - to surrender their full identity (through passport scans, facial recognition, or centralised databases) or whether they can prove only the relevant fact (that they meet an age threshold) and nothing else. ZKPassport enables the latter: a cryptographic proof of age derived directly from a government-issued document, with no personal data transmitted to or stored by the service provider. This positions the technology at the intersection of this Consultation's objectives and the broader digital identity agenda, and it is this intersection that this response addresses.

2. THE CASE FOR PRIVACY-PRESERVING DIGITAL IDENTITY

2.1 The introduction of any age verification system raises fundamental questions about the relationship between the state, technology providers, and citizens, particularly children. While age verification infrastructure, properly designed, can unlock significant benefits in protecting

---

[1] **Note**: https://www.gov.uk/government/news/landmark-consultation-seeks-views-on-major-measures-to-protect-children-on-social-media-gaming-platforms-and-ai-chatbots

children from harmful online content, history demonstrates that identity systems introduced for limited purposes tend to expand in scope, creating risks to civil liberties and privacy that persist long after the original justification has passed. This is sometimes referred to as 'function creep': a system designed to check whether a user is over 13, 16, or 18 could, if built on data-heavy foundations, become a tool for tracking every site a citizen visits and every service they access. Any new age verification framework must therefore be designed so that privacy protections are structural and technical, embedded in the architecture itself, rather than dependent on policy commitments alone.

2.2 The architecture of any age verification system matters more than the policy rhetoric that accompanies it. A system designed in haste, with citizens' data pooled in central registers and accessed at the state's convenience, will erode privacy regardless of whoever happens to be in office. Function creep is not a flaw in such a system but its natural condition. A system designed deliberately, with cryptographic guarantees, data minimisation and the keys to a citizen's credentials in their own pocket rather than in the hands of government or its contractors, can deliver the child safety the government promises without the surveillance it disclaims wanting. ZKP technology provides exactly this guarantee: citizens can prove facts about themselves (such as their age) without revealing any underlying personal data, and without that data ever leaving their own device. Critically, even if a future government were to seek to expand the scope of age verification requirements, the technical architecture itself would prevent it from being repurposed as a tool for mass surveillance or disproportionate data collection.

2.3 ZKPs are one of several privacy-enhancing technologies ("**PET**") that could play a role in age verification. However, ZKPs offer material advantages over other PETs, particularly in terms of their production readiness, interoperability with existing government infrastructure, and ability to provide cryptographically guaranteed data protection. We set out further context on ZKPs, and their proposed utility within the age verification framework, below.

3. BUILDING ON EXISTING GLOBAL STANDARDS

3.1 The UK does not need to design a digital identity infrastructure from scratch. The ICAO 9303 standard already provides a globally interoperable framework for electronic identity document authentication, relied upon by over 150 countries for e-passport gate systems. Every ICAO 9303-compliant electronic passport and national e-ID card stores the holder's date of birth as a digitally signed data element on its NFC chip. This means that the document itself, issued and cryptographically signed by the holder's government, already contains the information needed to determine whether a person meets any given age threshold. ZKPassport exploits this existing infrastructure: it reads the chip, verifies the government's digital signature to confirm the document is genuine and unaltered, and then generates a zero-knowledge proof that the holder is over (for example) 13[2], 16, or 18, without ever transmitting the date of birth, or any other personal data, to the requesting service. No new identity documents, no new databases, and no new issuance infrastructure are required; the building blocks are already in citizens' pockets.

3.2 The ICAO 9303 global standard began with the ICAO's Technical Advisory Group on Machine Readable Travel Documents, which was established in 1984, building on the 1980 standardisation of the Machine-Readable Zone. However, it was the post-9/11 security environment that produced binding international consensus. The 2003 New Orleans Resolution selected facial recognition as the globally interoperable biometric, and the United States used its Visa Waiver Program ("**VWP**") as leverage, under the Enhanced Border Security and Visa Entry Reform Act of 2002, VWP countries had to issue 9303-compliant biometric passports by 2006 or lose visa-free access. Belgium issued the first compliant ePassport in 2004; ICAO then extended the mandate to all member states by 2010, with non-compliant documents losing validity in 2015. The lesson is that international convergence on a single identity standard is not only achievable but already accomplished, under harder conditions, against stronger sovereignty objections, and within roughly a decade of serious effort. There is no need for the UK to reinvent the wheel.

3.3 ZKPassport is built directly on the ICAO trust chain (Country Signing Certification Authority, Document Signer, and chip data), the same cryptographic infrastructure that underpins immigration systems worldwide. This means that ZKPassport's identity verification carries the same level of assurance as a check at an e-passport gate, while adding the privacy benefits of zero-knowledge cryptography on top[3].

---

[2] **Note**: while all UK citizens (including children) have access to an ICAO compliant UK passport, children may be less likely to hold a UK passport (and will also not have the ability to hold a UK driving licence). In the interest of inclusivity (i) children's access may need to be managed entirely by a parent/guardian on a child's behalf, for example by their parent/guardian providing a proof of consent through themselves verifying their age and name, which may need to align with the last name of the child and/or (ii) an ICAO 9303 compliant physical identity card may need to be issued to children (as part of the UK's broader ID development) to ensure children themselves can access services, without having to rely on their parents / guardian.

[3] **Note**: with modern cryptography and technology it is possible to take any existing ICAO compliant ID (including UK passports and driving licences) and turn them into digital ID's that are opt in and privacy preserving.

3.4 Internationally, the direction of travel is clear. The European Union Digital Identity ("**EUDI**") Wallet project, the reference implementation of eIDAS 2.0, is being built with age verification as a cornerstone use case. Importantly, the EUDI project's public GitHub repository includes a demo age verification component that uses Noir (Aztec Labs' open-source programming language) and Aztec's open-source zero-knowledge circuits, taken from ZKPassport's open-source library, for its zero-knowledge proof implementation. Aztec Labs has not (yet) been formally engaged by the EU on this, but the adoption of Noir and ZKPassport's circuits in the EUDI project's codebase speaks to the maturity and suitability of the technology. We are proud that our cutting edge and future proof technology 'Made in Britain' is being utilised by the EU. The EU's age verification app is now in pilot with seven front-runner Member States (France, Denmark, Greece, Italy, Spain, Cyprus and Ireland), with the architecture explicitly using zero-knowledge proofs over passport / ID data, matching completed on the user's device, and no personal data sent to any external server. All 27 Member States are due to offer EUDI Wallets by end of 2026 under eIDAS 2.0.

3.5 For the UK government, the practical implication is straightforward. The cryptographic standards, open-source tooling, and production-tested infrastructure needed to deliver a privacy-preserving age verification system already exist and are in use. Importantly, they are 'Made in Britain'. ZKPassport is operational today, supports identity documents from over 130 countries, and its cryptographic backend (built on Noir) can be upgraded seamlessly as the technology evolves (to make it faster / more secure). By building on ZKP technology and the ICAO standard, the UK can move quickly, reduce development cost and risk, and ensure interoperability with international partners, rather than incurring the expense and delay of designing a bespoke solution.

3.6 For readers less familiar with the underlying technology: ZKPs are cryptographic techniques that allow one party (the 'prover') to demonstrate to another party (the 'verifier') that a given statement is true without revealing any information beyond the truth of the statement itself. Although the underlying mathematics has existed for over 40 years, recent breakthroughs have made ZKPs practical for everyday applications, including age verification, digital identity verification, and regulatory compliance checks. In the context of age verification, ZKPs enable a citizen to prove, for example, that they are over 13, over 16, or over 18, without revealing their date of birth, passport number, or any other personal data to the service provider.

4. HOW ZKPS CAN DELIVER THE CONSULTATION'S OBJECTIVES

4.1 When it comes to the proposed age verification framework, we think ZKPs are the best technology available to protect user privacy and maximise data security while still delivering on the government's goal of keeping children safe online. Beyond the privacy benefits (and the boost to public confidence that comes with them), ZKPs can also drive real operational efficiencies across the platforms that must comply.

4.2 To unlock these benefits, the government's approach to age verification needs to be open to integrating privacy-enhancing technologies rather than locking in traditional, data-heavy approaches to identity verification. The framework should let technology providers use ZKPs to meet the required age assurance standards. The existing UK digital identity and attributes trust framework and the digital verification services ("**DVS**") ecosystem provide a natural starting point for this, as does the government's own acknowledgement in the Consultation that age assurance methods must be accurate, trustworthy, easy to use and hard to bypass.

4.3 This section looks at the practical benefits of using ZKPs for age verification, organised around three themes: (i) trust, privacy and data minimisation (addressing the Consultation's requirements that age assurance be 'privacy-preserving and data-minimising' and that trust in privacy practices is vital); (ii) effective, proportionate and interoperable (addressing the requirements that age assurance be 'reliable, accurate, robust and effective', proportionate to the risk, and accessible across platforms); and (iii) solving age verification. (addressing the requirement that solutions be 'responsive to emerging technology and risk' and resistant to circumvention). Taken together, these benefits make a strong case for embedding ZKP technology in the UK's age assurance architecture.

Trust, Privacy and Data Minimisation

4.4 The Consultation recognises that age assurance methods must be privacy-preserving and data-minimising, and that trust in the privacy practices of age assurance technologies is vital for ensuring people feel safe using them. We couldn't agree more and we think ZKP technology is the most effective way to make good on that commitment. An age verification system rooted in zero-knowledge cryptography would let users control not just their data but their privacy in a way traditional approaches simply can't match. Instead of asking users to hand over personal data to be stored in centralised databases (creating 'honeypots' that invite cyberattack), a ZKP-based system lets users prove facts about themselves through cryptographic proofs, without the underlying data ever leaving their device. This approach is naturally aligned with the data minimisation principles in the UK GDPR, the ICO's Age-Appropriate Design Code, and the Consultation's own principles for age assurance. ZKPs provide the most advanced form of data minimisation available for age verification: rather than transmitting personal data, they allow users to prove a single fact (e.g., 'I am over 13', 'I am over 16', 'I am over 18') without revealing any underlying data. No personal data is transmitted, stored, or processed by the service provider at any stage.

(a) ZKPassport is a production-ready example of this in action. It works entirely on-device, generating selective-disclosure proofs that service providers can verify without ever storing, transmitting, or touching the underlying identity data. It uses the same ICAO open standards infrastructure relied on globally in airports and border systems to authenticate electronic identity documents, and can confirm that a facial liveness check matches the biometric data stored in a document's NFC chip, proving 'the person presenting is the document holder' without revealing the actual face data. The result is state-grade assurance, anchored in official government-issued certificates and biometric-match attestations, with user-controlled, self-custodial privacy. Critically, ZKPassport is fully open-source and does not need any intermediary to check someone's passport and issue new credentials: all you need is your phone and an ICAO-compliant document (an electronic passport, national e-ID card, or electronic residence permit). ZKPassport's cryptography backend is built using Noir, Aztec Labs's programming language, the same language and open-source circuits now appearing in the European Union's EUDI Wallet age verification pilot (as discussed further in section 3 below). The system is anchored on Ethereum, the most secure and trusted blockchain infrastructure in the world, providing a decentralised, tamper-proof foundation for identity attestations.

(b) The Consultation also acknowledges that age assurance requirements may mean adults being required to verify their age to access services, and that this could create trade-

offs to user privacy and friction with adults' online experiences. ZKP technology addresses this tension directly: users are not passively enrolled into a surveillance architecture but actively generate and present cryptographic proofs on their own terms, from their own devices. Adults who must verify their age to access services should not have to sacrifice their privacy to do so, and the system should not create the infrastructure for tracking which platforms any individual uses. In an era of growing privacy awareness and increasing national security risks (with citizens' data being leaked), amplified by the data risks associated with large-language models and autonomous agents, a ZKP-based approach ensures that privacy protection is baked into the technology, not just promised in policy documents.

4.5 *Effective, Proportionate and Interoperable*

(a) The Consultation identifies that improving how age checks work across different services, for example making them more interoperable or enabling device-level options, would make protections simpler to apply and easier for parents and carers to trust. ZKP technology can play a transformative role here. ZKPs enable reusable, portable age credentials: a single cryptographic proof generated on a user's device can be verified by multiple service providers without the user needing to undergo a separate age check with each one. This dramatically reduces friction for both users and platforms, enabling automated verification and eliminating the need for each service to build and maintain its own age verification infrastructure.

(b) The Consultation notes that Ofcom estimates 7.8 million UK visitors per day already access adult services with age assurance, and that current techniques are generally effective at distinguishing adults from under-18s. However, the Consultation also acknowledges that fewer solutions are currently available to distinguish a 14 from a 16-year-old, and that there are challenges to further age assurance adoption including privacy concerns and proportionality. ZKPassport is exactly the kind of technology that can address these challenges within the existing ecosystem: because it is open-source and self-custodial, users keep full control of their identity data on their own device, while service providers can verify cryptographic proofs knowing they meet the required standards. ZKPassport can generate proofs at any age threshold, making it suitable for the age-graduated restrictions the Consultation envisages.

(c) On top of that, ZKPs address the Consultation's concern about proportionality. The Consultation notes that the implications of a 13-year-old having screentime limits designed for 15-year-olds are different to the implications of a 13-year-old accessing pornography, and that age assurance must be proportionate to the restriction being enforced. ZKP-based age verification is inherently flexible: ZKPassport can generate proofs for any age threshold (over 13, over 16, over 18) from the same underlying credential, meaning platforms can implement age-graduated restrictions without imposing disproportionate verification burdens on users. The same proof architecture works whether the context is a minimum age for social media, a higher threshold for accessing risky functionalities, or an age gate for AI chatbot features. The Consultation also identifies that children with special educational needs and disabilities (SEND) may be particularly affected by restrictions, and that any approach must consider disparities in the online experiences of different groups of children. A ZKP-based system protects all users equally by default: because no personal data is disclosed during verification,

there is no risk of a child's details being exposed through data breaches, system errors, or unauthorised access, and no risk of data being used to build behavioural profiles of minors.

(d) ZKPs also tackle circumvention head-on, a major concern highlighted in the Consultation. The Consultation notes that VPN usage more than doubled in the UK following highly effective age assurance requirements becoming mandatory, and that many children are technologically savvy and likely to be aware of ways to bypass new rules. A ZKP-based age verification system is inherently resistant to common circumvention methods: because proofs are generated from the NFC chip data in a genuine government-issued passport or e-ID card, they cannot be forged, shared, or fabricated. Unlike self-declaration or simple date-of-birth entry, a ZKP proof provides cryptographic certainty that the person presenting it holds a valid identity document confirming they meet the required age threshold. This represents a step-change in the robustness of age assurance.

A Comprehensive Approach to Age Verification

4.6 A well-designed ZKP-based age verification system has the potential to transform how the UK protects children online. Over the last three years, a wave of regulation has turned age verification from a 'nice to have' into a legal mandate. In the UK, the Online Safety Act 2023 requires 'highly effective age assurance' for adult content and a widening list of social features, enforced by Ofcom with real financial penalties. This Consultation goes further still, with a statutory minimum age for social media, a higher age of digital consent, more robust age assurance mechanisms, and new age-related obligations on AI chatbots all on the table at once. In the EU, the Digital Services Act obliges platforms to protect minors, and the eIDAS 2.0 framework has put the EUDI Wallet on the critical path, with age verification as a cornerstone use case. In the US, the Supreme Court upheld Texas's age verification law in *Free Speech Coalition v. Paxton* in June 2025, and more than a dozen other states have introduced similar requirements. Australia has legislated a social media ban for under-16s. The question is no longer *whether* to verify age, but *how* to do so effectively without compromising privacy.

(a) Traditional age verification methods are not fit for this new regulatory reality. Self-declaration is trivially bypassed. Document-based checks (requiring users to photograph a passport or driving licence for server-side review) can be compromised through forged or borrowed IDs and create a toxic byproduct: a centralised database of verified government IDs. In October 2025, photographs of government IDs belonging to approximately 70,000 Discord users were exposed after a breach at verification vendor Persona. Biometric age estimation (where a selfie returns an estimated age range) avoids document collection but degrades in accuracy at the age boundaries that matter most (roughly 16 to 25), and some users object to biometric data being processed at all. The structural flaw shared by all legacy methods is over-disclosure: each one forces users to reveal substantially more about themselves than the question requires.

(b) ZKP-based age verification is designed to change that, answering only what is asked and learning nothing more. With ZKPassport, a citizen scans the NFC chip in their passport or e-ID card with their phone, and the app generates a cryptographic proof that they are over 18 (or any other required age threshold), without revealing their date of birth, name, or any other personal information. The service provider can verify the

proof instantly, with cryptographic certainty, without ever accessing or storing any personal data. This is not theoretical: it is technically proven and operational today. The French Data Protection Authority (CNIL) has acknowledged zero-knowledge identity as a privacy-friendly model for online age verification, and the EU's own age verification pilot (discussed in section 3 above) uses the same zero-knowledge approach that ZKPassport has been running in production. Privacy-preserving approaches will dominate over time, because the alternative, a centralised database of verified government IDs attached to every platform anyone uses, is both a security liability and politically unsustainable.

(c) ZKPassport's age verification works across both Web2 and Web3 environments, making it a good fit for the full range of private sector use cases the Consultation has in mind, from purchasing age-restricted goods in shops to accessing age-restricted services online. Importantly, ZKPassport does not require any eyeball scanning or collection of personal biometric data; it works directly with legitimate government-issued document data, without revealing anything beyond the specific attribute being proved. Interoperability will matter more than any individual vendor in this space: the platforms that will succeed are those whose age proofs can be reused across the web. ZKPassport's architecture is designed for exactly this, and the same proof can be reused across many services without compounding the exposure of any one of them. A comparison of ZKPassport against other leading digital identity technologies (including traditional KYC providers and the EUDI Wallet) is set out in *Annex 1* to this response.

TABLE 1: HOW ZKPS ADDRESS KEY AGE VERIFICATION CONSULTATION OBJECTIVES

For a broader view of how ZKPs can support the Consultation's key objectives, *Table 1* below maps ZKP capabilities against the main use cases and challenges identified in the Consultation.

Consultation Objective	**Description / Challenge**	**How ZKPs / ZKPassport Can Help**
Age Verification for Social Media and Online Services		
The Consultation proposes a statutory minimum age for social media (at least 13, potentially 16), alongside a requirement for this to be effectively enforced. It also considers age-restricting specific risky functionalities (livestreaming, disappearing content, location sharing) for children below a certain age. Highly effective age assurance is identified as critical to making any age-based restrictions workable.	Traditional age verification methods are not fit for this regulatory reality. Self-declaration is trivially bypassed by children. Document-based checks create privacy risks and centralised databases of government IDs. Biometric age estimation degrades in accuracy at the boundaries that matter most (13–16), and the Australian Age Assurance Technology Trial confirmed that facial estimation is less accurate for younger users. No single method works perfectly for all users in all contexts.	Using ZKPassport, a citizen scans the NFC chip in their passport or e-ID card and generates a ZKP that they are over 18 (or any other required age threshold) without revealing their date of birth, name, or any other personal information. The proof is generated on-device and can be verified instantaneously by service providers without accessing or storing any personal data. This is the most privacy-preserving age verification method available and is already operational.
Protecting Children from AI Chatbots		
The Consultation identifies that AI chatbots pose emerging risks to children including emotional dependence, parasocial attachments, and exposure to harmful content. It proposes minimum age restrictions and/or restricting access to certain chatbot features and functionalities for children. Services not currently in scope of the Online Safety Act will be brought under new duties.	AI chatbot providers need reliable age assurance to enforce age-based restrictions on features such as romantic roleplay, persistent memory, and anthropomorphic interaction patterns. Current methods (self-declaration, email verification) are trivially bypassed. The dynamic and personalised nature of chatbot interactions makes content-based moderation alone insufficient; access controls based on verified age are essential.	ZKPassport enables AI chatbot providers to verify a user's age with cryptographic certainty before granting access to age-restricted features, without collecting or storing any personal data. The same proof architecture works whether the restriction is a minimum age for account creation or a graduated threshold for specific features (e.g., over 16 for romantic interaction modes). Because verification is on-device and instant, it does not disrupt the user experience or require chatbot providers to build their own verification infrastructure.
Privacy-Preserving Compliance / Data Minimisation		

Consultation Objective	Description / Challenge	How ZKPs / ZKPassport Can Help
The Consultation emphasises that age assurance methods must be privacy-preserving and data-minimising, and that trust in their privacy practices is vital. The Australian eSafety Commissioner's guidance states that steps taken should be 'privacy-preserving and data-minimising' and should not rely on 'disproportionate amounts of information being submitted by users'. The ICO's Age-Appropriate Design Code reinforces this for children's data.	Most existing age verification methods require users to share personal data with third-party providers: uploading photographs of identity documents, submitting selfies for biometric estimation, or sharing behavioural data for age inference. Each method forces users to reveal substantially more about themselves than the question ('are you over X?') requires. Users must verify their age with multiple services, via different providers, compounding privacy exposure as they move across the internet.	ZKPs provide the most advanced form of data minimisation available for age verification. Rather than transmitting personal data, ZKPs allow users to prove a single fact (*e.g.*, 'I am over 13', 'I am over 16', 'I am over 18') without revealing *any* underlying data. No personal data is transmitted, stored, or processed by the service provider at any stage. The same proof can be reused across many services without compounding the exposure of any one of them. This goes beyond selective disclosure to achieve genuine zero-knowledge verification, fully aligned with the principles set out by both the Consultation and the Australian eSafety Commissioner.
Preventing Circumvention		
The Consultation identifies circumvention as a critical challenge. VPN usage more than doubled following highly effective age assurance requirements becoming mandatory. Children are technologically savvy and aware of ways to bypass rules, including using someone else's account, switching devices with siblings, and using VPNs. The Consultation seeks views on how to ensure age restrictions are as robust as possible.	Self-declaration and simple date-of-birth entry are trivially bypassed. Facial age estimation can be fooled with filters or photographs. Account sharing and device switching allow children to use adults' verified sessions. VPNs can be used to access services in jurisdictions with weaker age assurance requirements. No single legacy method provides cryptographic certainty that the person presenting is genuinely above the required age.	ZKP-based age verification is inherently resistant to circumvention. Proofs are generated from the NFC chip data in a genuine government-issued passport or e-ID card and are cryptographically bound to the holder through a biometric liveness check. They cannot be forged, shared, or fabricated. A ZKP is mathematically unforgeable: it is impossible to create a valid proof without holding the genuine underlying credential. Even if a child gains access to a parent's device, the biometric-match attestation prevents them from using someone else's proof. This fundamentally changes the circumvention landscape.
Interoperability Across Platforms		
The Consultation identifies that users often must verify their age with multiple online services, via different third-party age assurance providers, as they move across the internet. It seeks views on how to improve interoperability,	Current age verification is fragmented: each platform uses its own provider, requiring users to undergo separate checks on every service they access. This creates privacy	ZKPassport's architecture is designed for cross-platform interoperability. A single cryptographic proof generated on the user's device can be verified by any service

Consultation Objective	Description / Challenge	How ZKPs / ZKPassport Can Help
including device-level options and cross-platform verification. The Australian eSafety Commissioner encourages ‘successive validation’ using multiple age assurance methods in succession.	fatigue, increases the total volume of personal data shared across the ecosystem, and places disproportionate burdens on both users and smaller platforms that lack the resources to build bespoke verification systems.	provider without that provider needing to integrate with a specific third-party verification vendor. The same proof can be reused across many services without compounding privacy exposure. ZKPassport works at the device level (available on iOS and Android), meaning it can serve as a universal age verification layer across the ecosystem. This also supports the ‘successive validation’ approach: ZKPassport can serve as the highest-assurance layer in a multi-step process, providing cryptographic certainty where other methods are inconclusive.

TABLE 2 – RESPONSES TO THE CONSULTATION

Chapter	*Consultation Question*	*Aztec Labs / ZKPassport Response*
Chapter 2: Interventions for safer, more positive experiences	*Q4 – Would you support a legal requirement for social media services to have a minimum age of access?*	No. However, if any such requirement is introduced, the effectiveness and public acceptability of any minimum age requirement depends on the age assurance mechanism used to enforce it. A minimum age backed by privacy-preserving age verification (such as ZKP-based methods) avoids the trade-offs to adult user privacy that the Consultation identifies as a concern and provides cryptographic certainty rather than relying on self-declaration or estimation methods that children can easily circumvent.
	Q5 – To what extent do you agree or disagree with the following statement: "Social media services should have a minimum age of access of at least 16 and should not be accessible to any children under that age"?	Strongly disagree. In case any minimum age restrictions are introduced, the key variable is not the specific age threshold but the effectiveness of its enforcement. A minimum age set at any level is meaningless without robust age assurance to enforce it. ZKP-based age verification can generate proofs at any threshold (over 13, over 14, over 15, or over 16) from the same underlying government-issued credential, meaning the technical infrastructure is threshold-agnostic. Aztec Labs disagrees with setting any minimum age requirement; however, we note this is ultimately a policy judgment for the government to make. What we do advocate is that whichever threshold is chosen, it must be enforced through privacy-preserving technology that provides cryptographic certainty rather than relying on methods that create data honey pots for citizens, creating personal and national security risks.

Chapter	*Consultation Question*	*Aztec Labs / ZKPassport Response*
	Q10 – What should be considered to make raising the digital age of consent effective and workable?	If any minimum age restrictions are implemented, three factors are essential. First, robust age verification: raising the digital age of consent is only meaningful if platforms can reliably distinguish a 14-year-old from a 16-year-old. Self-certification mechanisms (tick boxes) are manifestly inadequate, as the Consultation acknowledges. ZKP-based verification provides cryptographic certainty because it works from official government-issued document data rather than estimation. Second, parental verification that is both reliable and privacy-preserving: where consent from a parent or carer is required, the verification process must confirm identity and parental responsibility without creating centralised databases of family relationships. ZKP technology can prove that a person holds a valid identity document and meets an age threshold, and future developments could support proof of parental responsibility through linked credentials. Third, inclusivity: the Consultation rightly notes that parents with less confidence or capacity to engage with digital processes may be disadvantaged, potentially widening digital inequalities. Any verification system must be simple, device-level, and accessible. ZKPassport works on standard iOS and Android devices with any ICAO-compliant identity document (a UK passport or UK driving licence), minimising barriers to access.
	Q15 – What do you think the impacts would be if some online services were required to introduce age restrictions on specific features and functionalities?	The impact on user privacy depends entirely on the verification technology used. If platforms implement feature-level age checks using data-heavy methods, users would face repeated privacy intrusions as they navigate different features within a single service. ZKP-based verification eliminates this concern: a single reusable proof generated on the user's device can be verified for multiple features without transmitting any personal data. The impact on business costs could be significant if each platform must build bespoke verification for each restricted feature; however, an open-source, device-level solution like ZKPassport can serve as a universal verification layer, dramatically reducing the engineering burden on individual platforms. The Consultation should consider the risk of fragmentation if platforms adopt incompatible verification methods, and should encourage interoperable, standards-based approaches.

Chapter	*Consultation Question*	*Aztec Labs / ZKPassport Response*
	Q29 - Should AI chatbots have minimum age restrictions?	If the government decides to implement any minimum age restrictions for AI chatbots, age verification using ZKPs provides the most effective and privacy-preserving way to enforce these restrictions. ZKPassport can verify whether a user is over 13, over 16, or over 18 with cryptographic certainty, enabling chatbot providers to implement graduated access controls without collecting any personal data from users. This is particularly important for chatbots currently out of scope of the Online Safety Act but which the government plans to bring under new duties.
	Q30 - What do you think the impact would be of introducing age restrictions on AI chatbots or certain features and functions?	If the government decides to implement any minimum age restrictions, ZKP-based verification means adults can prove they meet the age threshold without revealing any personal data to the chatbot provider, eliminating the privacy trade-off. The impact on business costs would be manageable: ZKPassport's open-source SDK can be integrated into chatbot platforms with minimal engineering overhead, and its device-level architecture means chatbot providers do not need to build or maintain their own verification infrastructure
Chapter 3: Effective compliance and enforcement of online safety rules	*Q31 - To what extent do you agree with this statement: "Adults should complete age checks more often, if it means children are safer online"?*	Strongly disagree. If any minimum age restrictions are implemented, any age checks ought to be privacy-preserving. The key barrier to public acceptance of age assurance is the privacy cost. If adults must verify their age to access services, the verification method must not create a record of which platforms they visit or expose personal data to service providers. ZKP-based age verification solves this: a user proves they are over 18 (or any other threshold) without revealing their date of birth, name, or any other personal information, and without the service provider learning anything beyond the binary yes/no answer. With ZKPassport, the privacy cost of an age check is effectively zero, meaning there is no trade-off between child safety and adult privacy. This should dramatically increase public willingness to accept more frequent age checks, despite our disagreement with such checks.

Chapter	*Consultation Question*	*Aztec Labs / ZKPassport Response*
	Q32 - What should be considered to make minimum age restrictions effective and workable?	Three factors are critical. First, **privacy by design**: any age assurance method must be data-minimising and must not create centralised databases of personal data. ZKP-based verification achieves this by ensuring no personal data ever leaves the user's device. Second, **proportionality**: the level of assurance required should match the risk. A ZKP proof can be calibrated to any age threshold (over 13, over 16, over 18) from the same underlying credential, enabling graduated restrictions without disproportionate burdens. Third, **interoperability**: users should not have to undergo separate age checks for every platform. ZKPassport's device-level architecture enables reusable proofs that work across services, reducing friction and improving both compliance rates and user experience.
	Q33 - What do you think the impacts might be from requiring age assurance across a greater number of online platforms?	The key risk is privacy, which is a critical personal and national security risk. If poorly designed age assurance is rolled out at scale, the result would be a surveillance infrastructure tracking which platforms every citizen uses. This is politically unsustainable and a national security risk (centralised databases of verified identities attached to platform usage are high-value targets for cyberattack by foreign adversaries). The key opportunity is child safety at scale. ZKP-based age verification eliminates the privacy risk entirely: no personal data is collected by any platform, so there is nothing to track, breach, or misuse. Importantly, this eliminates the personal and national security risk. Broader age assurance requirements become politically viable and publicly acceptable when the underlying technology guarantees privacy by design. The impact on business costs is also reduced: ZKPassport's open-source, device-level architecture means platforms do not need to build bespoke verification systems or contract with multiple third-party providers.
	Q34 - How, if at all, could age assurance be made more effective?	Age assurance can be made significantly more effective through three improvements. First, adopt cryptographic age verification (ZKPs) as the gold standard for high-assurance checks. Unlike facial age estimation, which degrades in accuracy at younger age boundaries, ZKP-based verification provides mathematical certainty because it works from official government-issued document data. Second, enable device-level verification so that a single proof can be used across multiple services, reducing friction and increasing compliance.

Chapter	*Consultation Question*	*Aztec Labs / ZKPassport Response*
		ZKPassport already operates at this level on iOS and Android. Third, support a 'successive validation' approach where ZKP-based verification serves as the highest-assurance layer in a multi-step process, providing certainty where estimation methods are inconclusive. The government should also ensure that age assurance standards explicitly recognise and certify ZKP-based methods within the existing trust framework.
	Q35 - What should be considered when assessing the effectiveness of age-verification and age-assurance technologies?	The following criteria should be central to any assessment: (i) **Privacy**: does the technology minimise data collection? The gold standard is zero-knowledge verification where no personal data is collected at all. (ii) **Accuracy**: does the technology provide certainty at all relevant age thresholds (13, 16, 18)? ZKP-based methods provide cryptographic certainty because they work from official document data, unlike estimation methods which degrade at younger boundaries. (iii) **Robustness**: how resistant is the method to circumvention? ZKP proofs bound to biometric liveness checks are mathematically unforgeable. (iv) **Interoperability**: can the same verification be reused across services? (v) **Inclusivity**: does the technology work for all users, including those without smartphones or identity documents? (vi) **Open-source and auditable**: can the technology be independently verified to work as described? ZKPassport meets all six criteria and is operational today.

Chapter	*Consultation Question*	*Aztec Labs / ZKPassport Response*
	Q40 - What should be considered to make age-restricting VPNs effective and workable?	We would strongly caution against (and frankly disagree with) age-restricting VPNs as a primary strategy. VPNs serve important legitimate purposes for both adults and children (protecting data on public WiFi, securing sensitive communications). The Consultation's own evidence shows that 66% of child VPN users use them to protect their personal data. **Rather than restricting a legitimate privacy tool**, which needs to remain freely accessible to use by anyone, if the government decides to implement any minimum age restrictions, the government should focus on making age assurance robust enough that circumvention via VPN is irrelevant. ZKP-based age verification achieves this: the proof is generated from a genuine government-issued document on the user's own device, so the user's geographic location (real or spoofed via VPN) is immaterial to the verification. If the government does consider VPN restrictions, any age check required should itself be privacy-preserving and use ZKP-based methods.

ANNEX 1 – COMPARISON OF AGE VERIFICATION TECHNOLOGIES[4]

	ZKPassport	Persona & Traditional KYC Providers	EUDI Wallet
		Overview	
Description	ZKPassport is an open-source identity verification solution that enables users to prove specific facts about themselves: age, nationality, personhood, without revealing any underlying personal data. It works by scanning the NFC chip embedded in a biometric passport or national ID using a smartphone, a private live face match, then generating a zero-knowledge proof entirely on-device. That proof can cryptographically demonstrate, for example, that the user is over 18, without disclosing their date of birth, name, or any other attribute.	Persona is a traditional identity verification platform for KYC, AML, and onboarding workflows. The product handles document checks, biometric liveness, and watchlist screening as a server-side SaaS. Users scan their documents and record the video of their face and upload to Persona servers where it gets verified and stored. There are other KYC providers like Sumsub, Entrust that work in a similar way.	EU-mandated digital identity wallet rolling out across all 27 member states. Each country issues its own wallet that meets common EU standards, so credentials work cross-border. Stores government ID, driving licence, diplomas, payment cards, and more. Supports selective disclosure of attributes; implementations may still reveal underlying data depending on credential format
Website	www.zkpassport.id	https://withpersona.com	https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/overview
		Core Architecture	
Core Technology	✅ Zero knowledge proofs	❌ Traditional identity verification (no ZK	🟡 Selective disclosure today via SD-JWT VC

[4] **Note**: The table is intended to serve as a general frame of reference, rather than an exhaustive description and comparison of each digital identity technology.

	ZKPassport	Persona & Traditional KYC Providers	EUDI Wallet
Future Proof	ZK-SNARKs (Noir circuits) over ICAO-standard eMRTD NFC chip signed data. All computation on-device. Verifier receives a math proof, never raw data. ICAO PKI → issuing state CSCA certificate → passport chip signature. Trust = you trust the state that issued a passport. Aligned with emerging privacy-first regulatory trends.	proofs) Document checks and face matching use Persona's closed-source ML models, supporting IDs from 200+ countries. All processing runs server-side. The verifying business gets the result plus, depending on its setup, the underlying personal data. ID issuer → Persona's servers → the business. Trust = you trust Persona, their security, and how the business handles your data. Aligned with current KYC/AML frameworks; evolving toward data minimisation,	and ISO mdoc proves specific facts (over 18, EU resident) without revealing the underlying document. Zero-knowledge proofs and BBS+ signatures (better unlinkability) are flagged in the spec as planned but not yet live. Future-proof in design intent, but the privacy-enhancing crypto isn't shipping in v1.
Issuer	Works with existing passports and ID cards issued by governments	Uses existing ID documents	Different levels of attestations issued by trusted providers - governments, universities, employers, etc.
Trust Anchor	Government PKI + Cryptography	Vendor Judgement	Issuer Signature
Open-source	✅ https://github.com/zkpassport	❌ Closed-source SaaS	✅Spec is open - https://github.com/eu-digital-identity-wallet
Use cases	Proof-of-personhood, age verification, sanctions screening, liveness check	Age verification, sanctions screening, liveness check	Age verification, custom credentials

	ZKPassport	Persona & Traditional KYC Providers	EUDI Wallet
Used in production	✅ Used by a couple organizations to verify age and uniqueness. Used by Aztec Foundation token sale to conduct sanctions screening..	✅ Used at scale by OpenAI, LinkedIn, Twilio, Square, Etsy, Gusto, and Udemy for KYC, age checks, and onboarding.	🟡 Pilots running in Germany, France, Italy, Spain, Netherlands, Sweden, Poland, and others. France Identité is being upgraded into an EUDI Wallet. Member states must offer wallets to citizens by December 2026, but most experts expect that deadline to slip for several countries. Real adoption is early
Onboarding	🟢 Works with any biometric passport or compatible national ID a user already holds, so onboarding is a one-time NFC scan on their own phone with no enrolment infrastructure required.	🟡 Onboarding is a guided document scan and selfie flow that works with the broadest range of IDs and the lowest hardware bar, but each integrating business runs its own onboarding so users repeat the process across services.	🟡 Each Member State stands up its own onboarding pipeline tied to national PID issuance, meaning users must re-onboard from scratch into a state-issued wallet even if they already hold a valid passport or national ID, and non-citizens/non-residents of the issuing state are excluded by design.
Interoperable between Web2 and Web3	✅ Proofs are easily verifiable both offline and with blockchain technology.	🟡 Strong Web2 integration via API, webhooks, and SDKs. Web3 support is limited to reading wallet risk data from Chainalysis and reusable KYC via Persona Connect. Verification still runs off-chain on Persona's servers and cannot be checked by a smart contract.	🟡 Strong Web2 interoperability designed for use across EU public services, banks, telcos, and online platforms. Web3 fit is unclear. The spec doesn't mention blockchain integration, and there's no clear path for using EUDI credentials in dApps today, though nothing technically prevents it.
Cross-border usability	✅ Global (passport-based)	❌ Vendor-dependent	🟡 EU

	ZKPassport	Persona & Traditional KYC Providers	EUDI Wallet
Privacy and Security			
Data Sharing Model	✅ Proof only. Eg: proof that the user is above 18 without revealing DOB	❌ Full document	✅ Selected attributes. Eg: only DOB.
Privacy from issuer	✅ Yes	❌ No	🟡 Likely yes, but implementations are pending.
User Control	✅ Users are in full control of their data and what they want to prove. User initiates every proof using their government ID. Data lives solely on their phone.	❌ The user submits documents and selfies through Persona's flow. The user does not hold the credential. Data retention is set by the business. Users can request deletion via the business.	✅ Users decide which credentials to share, with whom, and for what purpose.
Biometric Liveness	✅ Relies on a simple open-source (MIT licence) machine learning model for local private face matching, which helps ensure the liveness check is accurate and matches the person on the government issued ID.	✅ Selfie and video liveness using Persona's own ML, with gesture guidance and multi-frame analysis. Designed to defeat photos, masks, and deepfakes. Effective in production, though the model is closed-source and the check runs on Persona's servers, not the user's phone.	🟡 Liveness checks happen during initial enrolment to bind the wallet to the holder. Standards reference EU biometric and anti-spoofing requirements, but implementation is left to each member state, so quality will vary.
Age Verification			
Private	✅ Predicate-level disclosure - Users prove they are above 18 without revealing their exact DOB. The service learns literally only whether the user	❌ The service receives the verification result plus, depending on integration setup, names, dates of birth, document numbers, and other personal data. Persona itself sees all of it during	🟡 Selective disclosure allows users to reveal only DOB without revealing other credentials; but implementations might not have predicate-

	ZKPassport	Persona & Traditional KYC Providers	EUDI Wallet
	passes the age threshold.	processing. The user has no cryptographic guarantee that less data than required is shared with the business.	level disclosure.
Regulatory fit	✅ Architecturally fully aligned with data minimisation mandates in UK Online Safety Act, EU Digital Services Act, and US KOSA proposals. No behavioural profile created.	🟡 Strong fit with traditional KYC and AML rules (FinCEN, FCA, MAS) because that's what the product was built for. Less aligned with newer data minimisation laws, which favour systems that share less data.	✅ EUDI is the regulation. eIDAS 2.0 makes it mandatory across the EU by December 2026.