PAS 1296:2018

Online age checking – Provision and use of online age check services – Code of practice

EURIM DIGITAL POLICY ALLIANCE

bsi.

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

ISBN 978 0 580 91271 9

ICS 03.080.20

Contents

List of tables

Foreword

This PAS was sponsored by the Digital Policy Alliance (DPA). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on 19 March 2018.

Acknowledgement is given to Dr Rachel O'Connell of Trust Elevate Ltd, as the technical author and the following organizations that were involved in the development of the PAS as members of the Steering Group:

- AgeChecked
- Age Verification Providers Association
- Aristotle International
- Avoco
- Better Regulation Delivery Office
- British American Tobacco
- BSI Consumer & Public Interest Network
- Co-opted members
- Digital Policy Alliance
- ICM Registry
- Nicoventures, BAT Group
- Portland Broadcasting Ltd
- Trust Elevate
- Verime (Telecom2 Ltd)
- Yoti

Acknowledgement is given to the following organizations that provided additional funding to support the development of this PAS and provided technical input in its development.

- Brickchain Limited
- GBG PLC
- LexisNexis Risk Solutions

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a code of practice to be rapidly developed in order to fulfil an immediate need in industry. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Use of this PAS

It has been assumed in the preparation of this PAS that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Information about this document

Presentational conventions

The provisions of this PAS are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in italic type, and does not constitute a normative element.

Spelling conforms to *The Shorter Oxford English Dictionary*. If a word has more than one spelling, the first spelling in the dictionary is used.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a PAS cannot confer immunity from legal obligations.

0 Introduction

0.1 General

Broadly speaking, regulators, businesses and consumer groups seek to mitigate harm to customers, in particular children and young people. Legislative requirements concerning age-restricted products and services share the common objective of protecting the health, safety, and wellbeing of young people.

Businesses are also concerned with mitigating risks associated with either inadequate compliance systems or non-compliance and these include:

a) the possibility of criminal and disciplinary sanctions;

b) civil or criminal action against the business as a whole and individual partners; and

c) damage to reputation leading to a loss of business.

This PAS is written to assist those businesses that are mandated to comply with legal requirements in conducting age checks. It provides recommendations on the due diligence businesses can exercise to ensure that age check services deliver the kind of solution that meet a business's specific regulatory compliance needs.

Traditionally, to verify that an individual is, for example, 18+ years of age, the collection of a significant amount of personal data, including name, address, and date of birth, is required. In effect, age verification involves a full identity verification process. Recent technology and policy innovations in the electronic identity sector mean that it is now possible for age check services to check a single attribute of an individual's identity (i.e. age-related eligibility). For this reason the term "age checking" is used throughout this PAS to differentiate between traditional methods of age verification and those currently available on the market. "Age check services" is an umbrella term that includes both age check providers and age check exchanges that enable a range of business sectors to meet evolving legal, self- and co-regulatory requirements to establish an internet user's age-related eligibility to access content and services online. Age check services can meet the needs of a range of age-rated services that might require either a specific age or the age band into which a customer fits, which might be for instance over 18, or under 13 years of age. An age check elicits a yes/no response to a query, for example, is this person over 18 years of age or is this person below 13 years of age.

At the time of writing, both age check services and associated elements of an age checking ecosystem (e.g. certification bodies, assessors and auditors) are in the nascent stages of development. Therefore this PAS has been written to assist the range of key stakeholders involved in this ecosystem, including relevant regulators. It draws these stakeholders' attention to the principles that underpin the EU General Data Protection Regulation (GDPR) [1] to which both data controllers and processors are required to adhere. For example, Article 25 of GDPR outlines the "privacy by design" principle, which requires that data protection is designed into the development of business processes for products and services. It is important that both age check services and those that rely on their services implement measures that meet the principles of data protection by design and data protection by default. Measures could include the following.

- **Data minimization**, for example a data controller limiting the collection of personal information to that which is directly relevant and necessary to accomplish a specified purpose.
- **Transparency and consent.** The GDPR requires that valid consent is explicit for data collection and usage (see GDPR, Article 7; defined in Article 4). Moreover, data controllers are required to prove "consent" (opt-in), and consumers are required to be able to withdraw consent (Article 7; defined in Article 4). Consent for children below 13 or 16 years of age (the age threshold might differ in the member states)is required to be given by the child's parent or custodian, and needs to be verifiable (Article 8).
- **Pseudonymization** is an umbrella term for approaches like data masking that aim to protect confidential information that directly or indirectly reveals an individual's identity. Pseudonymization is a key concern of this PAS, which encourages the use of pseudonymization technologies. Article 4 of the GDPR explains that pseudonymized data "can no longer be attributed to a specific data subject without the use of additional information" , such as separately stored mapping tables. Where any such matching information exists, it is required to be kept separately and subject to controls that prevent it from being combined with the pseudonymized data for routine identification purposes. Data masking and hashing are examples of pseudonymization technologies.

This PAS highlights that age-related eligibility checks pose a question "Is this person over 18 years of age?", which elicits a yes/no response. That is, a customer's current age determines which services he/she is or is not eligible to access and it might relate to a single value (e.g. over 18) or an age range (e.g. between 13 and 17). Determining eligibility is therefore privacy-enhancing as it reduces the amount of personal data a relying party retains.

The GDPR introduces data protection impact assessments (DPIA) as a means to identify high risks to the privacy rights of individuals when processing their personal data. When these are identified, the GDPR expects that an organization formulates measures to address these risks. It is important that this assessment happens prior to the start of processing the personal data and focuses on topics like the systematic description of the processing activity and the necessity and proportionality of the operations. The UK Information Commissioner's Office has developed a checklist [2] which highlights 12 steps organizations can take now to prepare for the GDPR.

The provisions of the proposed e-Privacy Regulation [3] aim to regulate how businesses collect individuals' data online and enable internet users to have more control over tracking. The regulation applies to all "electronic communications content" and "electronic communications metadata" (i.e. a much broader set of information than "personal data", which is covered by GPDR). The proposed e-Privacy Regulation outlines substantial penalties for non-compliance.

The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) [4] aims to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. Internet users can use their verified electronic identities, for example, mobileID, BankID online, and avail of services that utilize electronic identifications (eIDs) to enable, for example, an age-related eligibility check. For more information about the use of national eIDs by the private sector, see **D.4.3**.

To future-proof this PAS, some of the recommendations contain aspirational elements that anticipate how this ecosystem might evolve. In tandem with the emergence of identity- and consent-based attribute providers, a number of consent management platforms are also proliferating. These platforms enable businesses to request, receive and capture customer consent to the use of their personal data. Both human- and machine-readable consent receipts are created which enable customer data rights management across data ecosystems. Typically, these platforms operate in accordance with open standards and protocols.

This PAS is not intended as a one-size-fits-all solution. It is recognized that businesses that are required to conduct age checks vary greatly according to the type of service, the platforms on which they can be accessed, their user demographics, the markets in which they operate and the jurisdictions in which they are based. All of these factors affect the levels and types of risks that are attendant to those services and the strategies that might be appropriate and reasonable in order to address such risks.

The GDPR imposes obligations on all data controllers and processors where processing relates to offering goods or services to, or monitoring the behaviour of, data subjects within the EU. This could affect not only how an individual organization, but also how those companies with whom it contracts, handles personal data.

For example: company X in Canada does business with an EU-based firm, company E. As part of this business there is an exchange of customers' personal data. Company E handles the personal data in keeping with the GDPR regulatory regimen. The individuals receive timely notifications of how their data is handled; they have say-so on how it can be shared. Company E with the data is obligated to protect it, and to hold those with whom they do business (company A and others) to honour the basis on which they have made the personal data sharing agreement with the individual(s).

If company X does business with company A in Canada or South America or Asia, and company A does not honour the GDPR regulations, it could therefore be out of compliance.

Accordingly, in determining their strategies, it is important that businesses take into account the particular nature of their services, consider data governance, risk mitigation and liability and recognize that age check services are both emerging and evolving when applying the recommendations. The benefits of adopting a risk-based approach include:

a) enhanced consumer protection, e-safeguarding and privacy;
b) more efficient and effective use of resources proportionate to the risks faced;
c) minimizing compliance costs and optimizing benefits for customers; and
d) greater flexibility to respond to emerging risks as the methods used to gain access to age-restricted goods and services evolve, which means that a business, or a sector, is able to focus its resources on the areas of greatest risk.

0.2 Purpose of this PAS

Public-facing service providers such as online vendors, sellers, importers or distributors selling age-restricted goods or services can use this PAS, which provides a benchmark for good practice.

The PAS enables both businesses and groups within society to mitigate risks to children and young people's wellbeing by preventing ineligible customers from:

a) buying age-restricted goods online;
b) accessing age-restricted online content, (e.g. streaming age-restricted media, adult content, specific categories of advertising);
c) using age-restricted online services (e.g. dating agencies); and
d) accessing harmful content on platforms and apps, (e.g. gaming social media and messaging).

This PAS gives recommendations for the public-facing service providers' own good practice as well as for the implementation of tools to check that the age-related eligibility data provided by age check services for each online user is acceptable for the websites that they are accessing.

Adherence to the recommendations given in this PAS could reduce the risk of a merchant unwittingly selling or providing services to those who are not of a specified age as well as protecting minors by preventing them from inadvertently or deliberately accessing websites containing for example, adult content.

Users of this PAS might be legally required to implement age checks or might choose to adhere to self-regulatory age checking measures in order to demonstrate social responsibility.

An organization that is legally required to conduct age checks and contracts with an age check service is referred to throughout this PAS as a relying party. A relying party might choose to use one of the following solutions.

Proprietary identity verification solution provided by a traditional identity provider that can verify age, which is an attribute of an individual's identity.

Age check provider, for example, a bank, utility company or a mobile operator that holds verified data about a large cohort of their customers and enables those customers to permit age checks. It may also be a traditional identity provider that has adapted their service offering and can, with the appropriate user consent, provide an age check service.

The properties of the identity evidence and the sources of the data that underpins the age checking process are important determinants of the vectors of trust score (see **4.4**) associated with the age check.

Technology based solutions. Technology innovation has led to the development of solutions that combine a number of technological capabilities, for example, optical character recognition (OCR), to enable a user to scan their photo ID documents to enable an age check. The properties of the photo ID issuance and the strength of the identity verification processes that underpin the ID, e.g. whether or not facial recognition was used or data was cross matched with data held by a credit reference agency, are important determinants of the vectors of trust score that can be placed in the age check (see **4.4**). Various standards provide indications of the amount of trust that can be placed in biometric analyses (see Annex A).

Age check data providers. Businesses that mine and analyse unstructured data from one or multiple sources to deduce the likely age band to which an Internet user belongs. Currently there are a number of late-stage start-ups that have developed solutions that, with a user's permission, will analyse that user's social media presence or online footprint to determine the likely age-band that user fits. In time, age check data providers will include, for example, social media companies and many types of big data service providers.

Age check exchanges, which supply age check services (see Annex B).

Crucially, new and emerging age checking services do not necessarily have to rely on cross-checking personal data against databases or traditional sources of identity evidence. The effect of a greater number of data sources is the emergence of an age check services marketplace that enables online businesses to meet legal requirements to limit children and young people's access to age-restricted content and services.

An outline description of this PAS is given in Figure 1.

Figure 1 – Online age checking key concepts

Online service user/consumer:

- consents to provide data or to the release of a token requested by the relying party (online service provider) for age checking purposes;
- the GDPR defines consent as "a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action signifies agreement to the processing of personal data relating to him or her" – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent is required to be separate from other terms and conditions, and the individual has the right to withdraw consent; and
- is afforded greater protection of their information rights both in the ordinary course of transacting online and in the event of a violation.

Relying party:

- uses the user data provided to undertake its age checking practice to meet its age checking policy (see Clause **3**);
- requires trust capability statements (see Clause **4**) for age check services it uses in order to select suitable age checking services:
  - data governance;
  - authoritativeness;
  - conformity with standards;
  - vectors of trust score;
  - trust framework;
  - privacy policies.

From a consumer protection perspective, it is important that the relying party ensures that the responsibilities of all parties within the data ecosystem align with both the GDPR and contractual obligations.

Age check services:

- categories:
  - age check providers
  - age check exchanges
- provide and keep up-to-date trust capability statements;
- undertake age checking processing when agreed user data is provided in an agreed format.

0.3 Policymaking, technological innovation and a risk-based approach

Brownsword (2012) [5] suggests that there are four different challenges facing policy-makers dealing with new technologies: the need for regulatory prudence, regulatory legitimacy, regulatory effectiveness and regulatory connection. In most circumstances, it would, for example, be self-defeating to require the introduction of protective measures with such a high economic cost that the company or industry would cease to be viable, but it would be equally self-defeating to introduce regulatory measures which were toothless and ineffective. To get this balance right, a risk-based approach that involves industry self-regulation is often preferred.

Two enduring principles underpin the UK's health and safety related regulation, as follows.

a) "Those who create risk are best placed to control that risk" [6] – this translates into a preference for an industry self-regulatory approach to managing risk rather than a more prescriptive, interventionist approach. In practice, emphasis is placed upon businesses conducting risk assessments, performing due diligence, adopting risk-based strategies and tools and being able to demonstrate to regulators the rationale that underpins their particular approach. A self-regulatory approach also has the advantage of reserving enforcement agency attention for those businesses that either have inadequate compliance systems in place or are non-compliant.

b) "All risks do not have to be removed, but the law requires duty holders to do everything 'reasonably practicable' to protect people from harm" [6] – the recognition that it is not possible to remove all risk also applies to age-related eligibility checks.

For example, while age checks might make it more difficult for young people to purchase knives, a small number of determined young people will inevitably circumvent the checks. However, those retailers that implement age checks will have done everything "reasonably practicable" to protect young people from harm. Moreover, many stakeholders have a role in maintaining or improving standards and the strategies put in place by businesses do not operate in isolation. For example, effective regulation of the sale of knives involves not only retailers, but it also requires the collaboration between local regulators and the police. Regulators value the intelligence that they receive from the police, which can inform the prioritization of businesses within the regulatory planning processes. Programmes of education and community engagement are also important factors in both reducing knife crime and creating safer communities. The efficacy of self-regulation and the use of age checks are best evaluated in the context of the full range of measures put in place by relevant stakeholders. Moreover, self-regulation also implies a process of re-examination of practices at regular intervals as levels of risk are constantly changing in response, in part, to the effects of various risk-based strategies, therefore the efficacy of regulation is best assessed over a period of time.

0.4 Age checking

Regulated public-facing service providers, for example, gambling operators and banks, carry the responsibility for verifying their customers' identities, to mitigate against the risk of fraud, money laundering and identity theft. For a more detailed discussion of identity and age verification, see Annex C.

In instances where an individual wishes, for example, to purchase alcohol or view adult content, there is no legal requirement to know anything other than that the person is aged 18 years or over. Instead, single attributes of an individual's identity can be checked, for example, age-related eligibility. The response to a check, for example, on whether a user is over 16 years of age, is yes/no, and a trust score is provided by the age check service, which indicates the level of trust that can be placed in the response. The response can also be tokenized, which is a process by which certain data components are substituted with a non-sensitive equivalent. That equivalent is called the token. The token has no exploitable value, but it serves as an identifier. It is a reference that traces back to the original data. If this response is tokenized for re-use, a vectors of trust score is supplied to subsequent recipient relying parties – see **F.3** on communicating vectors of trust.

In a federated model, a "verify once, use many times" approach can reduce the cost of an age check. In effect, new and emerging age check services aim to minimize the costs to businesses of conducting age checks and thereby complying with regulatory requirements.

The European Commission and the UK Government have proposed legislative changes (the Digital Economy Act 2017 [7] and proposed updates to the EU's Audio Visual Media Services Directive (AVMSD) [8]) designed to ensure that online businesses respect children's rights online. In particular, those enshrined in Article 17 of the *UN Convention on the Rights of the Child* (UNCRC) [9], which states:

> "States Parties recognize the important function performed by the mass media and … encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being ..."

The European Commission recognizes that children have particular needs and vulnerabilities on the internet; however, the internet also provides opportunities for children to access knowledge, to communicate, to develop their skills and to improve their job perspectives and employability. The European Commission's *A European Strategy to deliver a Better Internet for our Children* [10] proposes a series of actions to be undertaken by the Commission, member states and by the whole industry value chain. For example, the strategy proposes a series of actions grouped around the following main goals.

- Stimulate the production of creative and educational online content for children, as well as promoting positive online experiences for young children scaling up awareness and empowerment including the teaching of digital literacy and online safety in all EU schools.
- Create a safe environment for children through age-appropriate privacy settings, wider use of parental controls and age rating and content classification.
- Combat child sexual abuse material online and child sexual exploitation.

The evolving regulatory and policy environment dictates that the age band to which a user belongs is becoming increasingly significant in a range of instances. There is pressure mounting on online businesses to ensure that both age-restricted and age-rated online content, goods and services are only accessible and delivered to those for whom they are intended or legal.

Moreover, Article 8 of the GDPR [1] requires online businesses to obtain verifiable parental consent before processing the personal data of a child aged below 13 or 16 years of age (the age threshold might differ in the member states).

Technology and policy innovation mean that a range of privacy preserving, affordable age check services are emerging that can meet the needs of a wide variety of business sectors.

This PAS takes the approach of decoupling identity verification and age checking and only deals with age checking. It provides guidance and recommendations for businesses considering contracting with age check services. The twin aims of this PAS are protecting consumers and allowing those who deploy age check services to demonstrate good practice. Guidance on standards relating to electronic identity verification is provided in GPG 45, *Authentication and Credentials for use with HMG Online Services* [11].

This PAS assumes that identity and attribute federation technologies can be used to enable a verify once, use many times approach to age checks. Federation offers convenience to businesses and their customers respectively, and might have economic advantages. This PAS outlines that a federated approach is underpinned by a trust framework which is a new mechanism for achieving large-scale trust online that consists of two parts:

a) the tools – the technical standards and protocols to be implemented by the members of a trust community; and
b) the rules – the business, legal, or operational policies to be followed in order to achieve the level(s) of security, privacy, and other trust assurances that the participants in the trust framework desire.

This PAS recognizes that an online business required to conduct age checks (i.e. a relying party) can fulfil more than one role within an identity ecosystem, including an identity provider, age check provider or an age check exchange.

The focus of this PAS is expressly on age, which is just one of many attributes associated with an individual. However, in instances where a transaction requires the checking of additional attributes, many of the recommendations contained in this PAS will apply.

0.5 Existing and evolving approaches to age checking

A detailed overview of traditional age verification methods and related self- and co-regulatory measures employed, over the last two decades, by mobile operators, ISPs and UK-based adult content providers of TV like video-on-demand services alongside those used by retailers, online gambling operators and gaming platforms designed for young children, is given at Annex C. Figures 2–4 illustrate different approaches to age checking. It is important to note that there is a range of both established and start-up age check services available on the market. It is possible to contract with an individual age check provider, to access multiple age check providers via an age check exchange or a hybrid of these two models and it is important to conduct a due diligence process (see Figures 2–4).

Figure 2 – Traditional approach to age verification

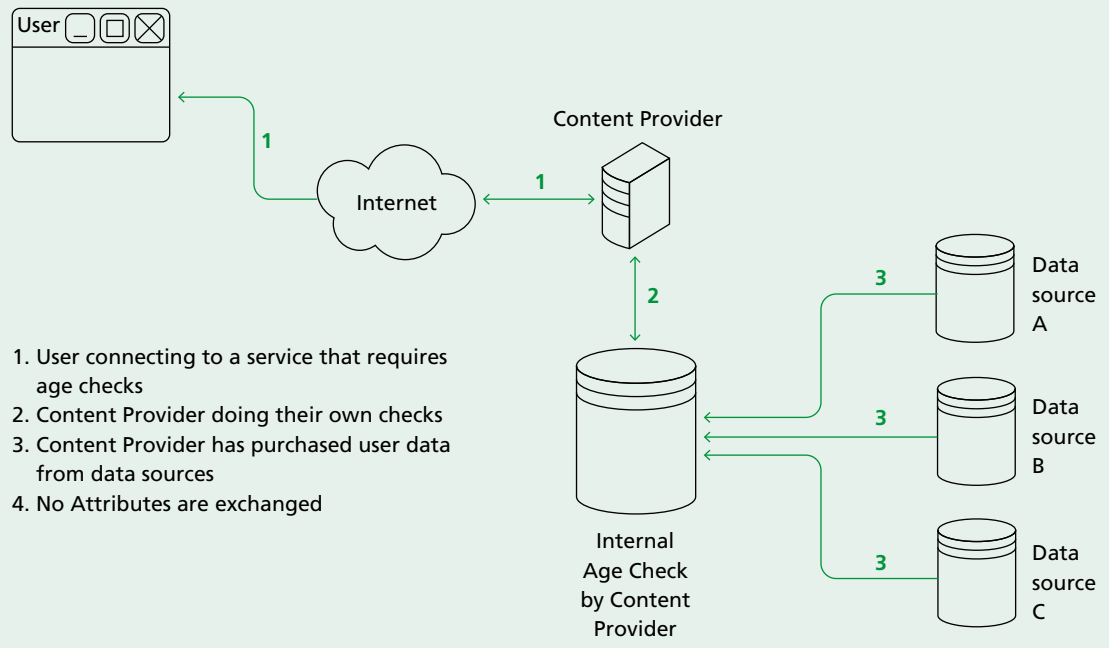


Figure 3 – Hybrid: traditional approach plus a minimal age check exchange

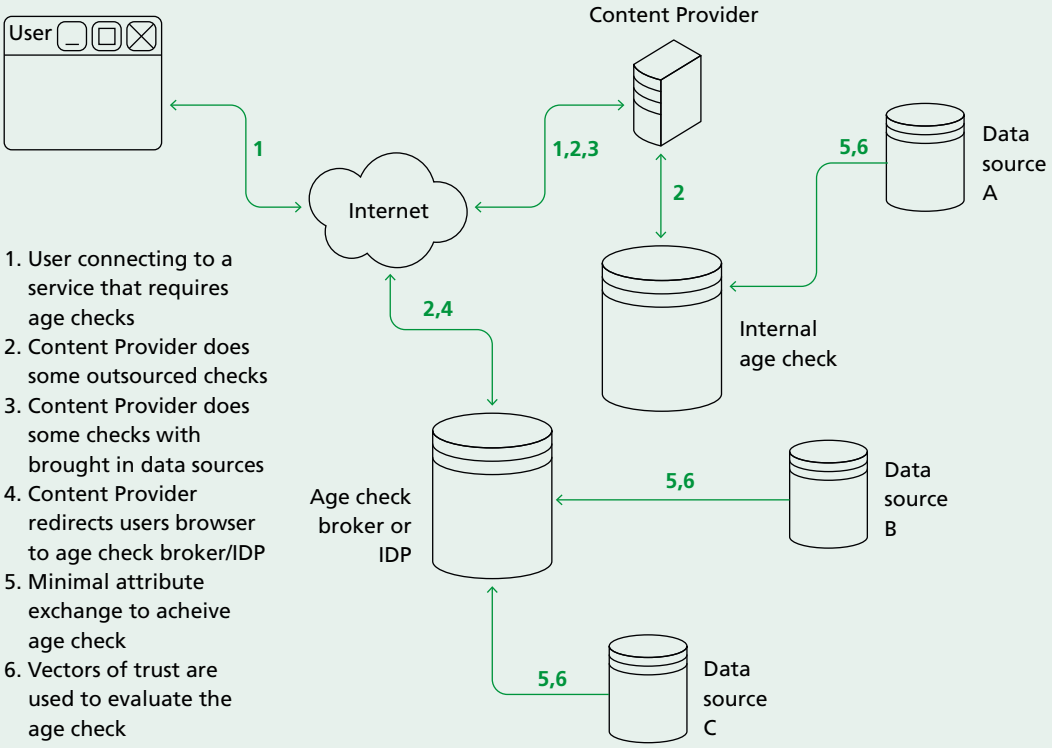
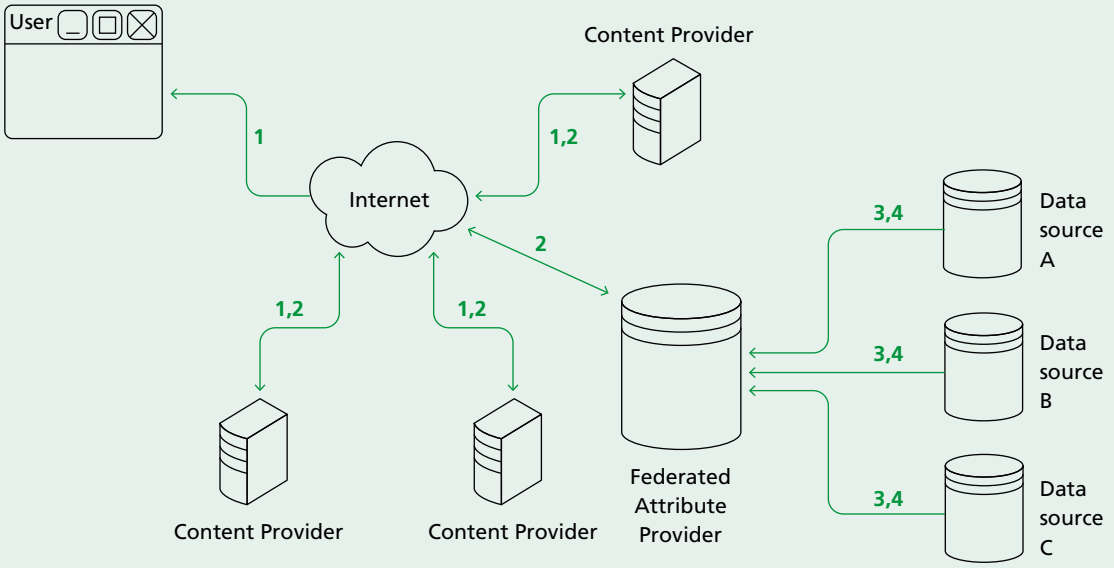


Figure 4 – Federated age check provider



1. User connecting to a service that requires age checks
2. Content Provider using federated age check scheme to verify age of the user
3. Minimal attribute exchange to acheive age check
4. Vectors of trust are used to evalutate the age check

Typically, traditional age verification methods oblige each business to conduct a level of customer due diligence (CDD) to collect a customer's personally identifiable information (PII), and cross-check it against identity databases to establish age. Businesses store verified PII, which not only carries privacy concerns but also poses a significant security risk, as this data is attractive to hackers (see Annex D).

Annex C also examines the UK Digital Economy Act 2017 [7], in particular the provisions relating to online pornography. It also explores the proposed updates to the European AVMSD in the context of the European Commission's *A European Strategy to deliver a Better Internet for our Children* [10].

Annex D juxtaposes the provisions of the existing data protection directive with those of the GDPR. It examines the implications of both the "privacy by design" principle and the extraterritorial reach of various articles, including Article 8, of the GDPR.

The UK's Information Commissioner's Office issued the following statement after the referendum result which indicated that the UK would leave the European Union.

> "The UK will continue to need clear and effective data protection laws, whether or not the country remains part of the EU. The UK has a history of providing legal protection to consumers around their personal data. Our data protection laws precede EU legislation by more than a decade, and go beyond the current requirements set out by the EU, for instance with the power given to the ICO to issue fines. Having clear laws with safeguards in place is more important than ever given the growing digital economy, and is also central to the sharing of data that international trade relies on."

D.4 explores the investment made by the European Commission, national governments and the private sector that has fostered the emergence of secure eID across Europe. It also examines the eIDAS regulation on electronic identification and trust services for electronic transactions in the internal market. Since each member state has a separate system to manage electronic identities, a mechanism was needed to make them comparable and interoperable. The eIDAS implementing regulation includes detailed criteria which allow the member states to map their eID means against a benchmark that measures the level of confidence one can have in the secure eID (low, substantial and high) and thus to compare each other. Other countries developing secure eID solutions, e.g. US National Strategy for Trusted Identity in Cyberspace (NSTIC), can also map to these levels of assurance.

The eIDAS regulation creates a predictable pan-European regulatory environment that enables secure and seamless electronic interactions between businesses, citizens and public authorities. Moreover, eIDAS enables age check services to leverage secure eID to meet the requirements of online businesses.

The confluence of regulatory drivers, legal, policy and technical enablers create the perfect conditions for the emergence of reliable, affordable, privacy preserving age check services.

0.6 Structure of this PAS

Clauses **3** and **4** provide guidance and recommendations for relying parties on determining their age checking policy and assessing the trust capability in an age check service. Trust capability statements assist relying parties in the process of assessing the amount of trust that can be placed in an age check service. A relying party decides what their requirements are for trust capability statements (see Clause **3**).

Trust capability statements assess the following.

a) **Data protection** (see **4.1**)**.** Relying parties hold a data governance policy for any age check services they use (see **4.1**).

b) **Authoritativeness** (see **4.2**)**.** Authoritativeness covers the quality and trustworthiness of the data on which an age check service relies. The authoritativeness category (0–3) informs a relying party's deliberations on the trust capability of the age check service. Designation of the authoritativeness of an age check service as one of the four levels can occur in various ways and is specific to the relationship between the relying party, age check service, and the legal authority governing the relying party.

c) **Conformity assessment** (see **4.3**)**.** This PAS advises relying parties and age-related eligibility services on the importance of age check services attaining a conformity assessment category concerning their data management, data quality, and security practices. This PAS identifies a range of standards that an age check service might be required to meet. The conformity assessment category of an age check service is important from the perspective of businesses conducting due diligence with respect to contracting with an age checking service. This PAS also covers the provision of an age check practice statement that an age check service can complete and to which a conformity assessment category can be ascribed.

d) **Vectors of trust** (see **4.4**)**.** Vectors of trust [12] combine attributes of the user and aspects of the authentication context into several values. A vector of trust score communicates the level of reliability in the processes leading up to and including the authentication process itself, thus providing assurance that the person associated with an age-related eligibility assurance (AREA) token is, in fact, the person to which the token was assigned. A vector of trust is also a function of the processes, management activities, and technical controls that have been implemented by an age check service.

e) **Trust framework**. Where a relying party is contracting directly with an age check service there is a contract governing their relationship, but where a relying party is using an age check exchange there is a trust framework in place which is legally binding on the participants to the age check exchange. It is important that the relying party is familiar with the constituent parts of a trust framework and the role of each party with respect to an age check exchange (see Annex B). A trust framework is a legal document that articulates the underlying legal structure of standards and policies that define the rights and responsibilities of participants in using an age check exchange. Through a trust framework a relying party specifies the business rules that determine which age check providers the relying party transacts with via the age check exchange.

Clause **6** covers the use of intelligent monitoring and customer support systems to detect attempts to game age check services.

Clause **7** covers recommendations for requesting metadata from age check services.

Clause **8** sets recommendations specific to the use of an age check exchange. This includes setting out criteria to assess the extent to which the age check exchange adheres to privacy and consumer protection principles (see Table 6).

1 Scope

This PAS gives recommendations for a framework for the provision and use of online age check services. This includes, for example. checking the age of those:

a) buying age-restricted merchandise online [e.g. e-liquids (nicotine), adult materials, dangerous goods];

b) accessing online content (e.g. streaming media, adult content);

c) using online services (e.g. dating services, gaming or gambling websites); and

d) enabling access to online age-gated material and services (e.g. education for minors and health for seniors).

NOTE 1 *This PAS is applicable to the use of both in-house and third party age check services.*

This PAS is written to assist those businesses that are mandated to comply with legal requirements to conduct age checks. It provides recommendations on the due diligence businesses can exercise to ensure that age check services deliver the kind of solution that will meet a business's specific regulatory compliance needs.

The PAS does not recommend any specific age checking tools for implementation.

This PAS gives recommendations for processes that can be applied when providing and using age check services in order to protect consumers and the online merchant or assist an organization that wishes to enable enhanced e-safeguarding.

NOTE 2 *See Annex A and Annex E for information about standards relevant to cryptography and the use of biometrics and other out-of-band methods.*

The audience for the PAS is:

a) any organization that wishes to use age check services to conduct age checking, including online merchants and service providers who deal with age-sensitive products; and

b) any organization providing age check services.

NOTE 3 *Regulators, professional bodies, trade associations, consumer protection groups, local authorities, and others can use this PAS as a resource. These organizations might have a legal, regulatory, supervisory, advisory, or enforcement role with respect the deployment of age check services by businesses, in one or more sectors. It is important to note that in regulated markets the regulator might establish key criteria as a minimum set of requirements to be met by age checking. The relying party can then decide whether they will go further than that, perhaps to differentiate themselves from others in the market.*

In markets with no regulatory age check requirements established, relying parties can use this PAS to determine for themselves the criteria and requirements their business would meet in order to undertake appropriate age checking.

NOTE 4 *Although consumers are not a primary audience for this PAS, the privacy, security and consumer protection mechanisms that ought to put in place by both age check services and the businesses they serve, are referred to throughout this PAS.*

This PAS does not cover recommendations for the checking of specific ages (e.g. 18+ years, 21+ years, <13 years, 65+ years), though the tools implemented might incorporate this.

This PAS is technology agnostic (i.e. it is unbiased towards the use of different technology tools to solve the age checking issue).