Technical Paper on Age Assurance

Federal Association of the Digital Economy (BVDW) e. V.
November 2026

Executive Summary

Age assurance is set to play an important role in protecting children and young people in the digital environment. However, numerous questions remain open regarding its specific design, technical implementation and integration into existing regulatory structures. The central question is how age limits and age-related safeguards can be implemented effectively without unduly restricting data protection, usability, digital participation and open access to digital services. This paper sets out the available methods, their technical foundations and the associated regulatory and practical requirements.

In line with the Commission proposal for an EU Kids Act, the paper uses **age assurance** as the overarching term. It covers various methods by which a person's age can be determined, estimated or verified. Mere self-declaration of age is to be distinguished from this. The paper differentiates between three fundamental methods:

- **Age verification relies on reliable evidence, such as an official identity document, identity information previously verified by a bank or a digital proof-of-age attestation. It can provide a reliable result, but usually involves greater effort and may entail the processing of sensitive personal data.**

- **Age estimation derives a person's likely age or age range from behavioural characteristics or facial features. It does not require proof of identity, but produces probabilistic results. Appropriate safety margins are particularly important close to relevant age thresholds.**

- **Age inference draws indirect conclusions about a person's age from information that is already available, such as contract, payment, account or mobile network data. It may be possible without any further action by users, but its reliability depends heavily on the quality and probative value of the information used.**

A distinction must be drawn between the method used and the result transmitted to a digital service. To make an age-related decision, the service generally needs neither the identity nor the exact date of birth of a person. An **age signal** that merely confirms whether a particular age threshold has been met or not is often sufficient. This separation between method, underlying data and transmitted result is of particular importance for a data-minimising design.

The methods differ in their level of assurance, the technical and organisational effort they require, their accessibility and their impact on data protection. No single method meets all requirements equally or fully prevents circumvention. Document-based methods can provide a high level of assurance, but require suitable identity documents. Age estimation is generally more accessible and less burdensome, but has inherent margins of error. Age inference can draw on existing data, but its reliability may be reduced by shared accounts, family mobile plans or payment methods belonging to someone else. The key question is therefore not simply which technology is chosen, but whether it is suitable for the intended purpose and how it fits into the wider system. Tiered or combined approaches may help offset the weaknesses of individual methods and reserve more stringent checks for uncertain cases or situations involving particular risks.

The Commission proposal for an EU Kids Act makes the permissibility of different age assurance solutions dependent on the purpose for which they are used. A method's regulatory suitability therefore cannot be assessed in the abstract, but only in relation to the specific use case and the level of assurance required.

A key challenge lies in separating age assurance from identification. Methods should enable an age-related determination without simultaneously disclosing users' identity, tracking their behaviour or linking data across different services. Three key design principles can be derived from the requirements of the EU Kids Act: the transmission solely of the required age attribute, the technical and organisational separation between the verifying entity and the service being used, and the use of cryptographic methods that allow an age threshold to be confirmed without disclosing the underlying identity data. In attestation-based age verification methods, these principles can be implemented with comparative technical clarity. In the case of estimation and inference methods, by contrast, it remains partly unclear how individual requirements, in particular the zero-knowledge proof principle, are to be implemented in practice. Here, on-device processing, the immediate deletion of input data and the exclusive disclosure of the result are of particular importance.

In future, the EUDI Wallet can become an important building block for the data-minimising provision of digital proof of age. It is intended to make it possible to present individual attributes such as "over 18" without disclosing identity or date of birth. Open standards are intended to ensure that such credentials can be used across providers, platforms and national borders. However, the wallet is not an immediately available or suitable solution for all users and use cases. Particularly during the transition phase, and for people without a wallet, a suitable device or available proof of identity, alternative means of access must remain in place. The parallel availability of different methods is therefore relevant both for practical feasibility and for digital inclusion.

The methods and requirements examined point to a risk-based, tiered approach. The level of assurance required should reflect the specific risk posed by a service, item of content or feature. Particularly high-risk services may call for more robust methods, while less demanding methods may be appropriate where risks are lower. Wherever possible, age assurance should be applied at the point where a specific need for protection arises, for example when accessing 18+ content, sending direct messages to unknown people, using live-streaming features or making in-app purchases. A uniform level of checking across all services and features would fail to reflect the different risks and contexts of use.

The size of the group of users affected by a check is also significant. The more extensively age assurance becomes a precondition for access to digital services, the greater the associated burden on adults as well. A higher level of protection must therefore not automatically be equated with a more extensive collection of personal data.

Regulatory requirements should be based on clear quality and effectiveness criteria and should be sufficiently technology-neutral. Open and interoperable interfaces can prevent individual providers, operating systems or technical infrastructures from being permanently favoured. At the same time, clear and workable requirements are needed so that small and medium-sized enterprises can also implement such solutions. As digital services are regularly offered across borders, a coordinated European approach is preferable to divergent national approaches. Differences between national requirements increase implementation costs, create legal uncertainty and can lead to inconsistent levels of protection.

Finally, age assurance should be understood as one building block of a more comprehensive approach to child and youth protection. It can provide technical support for age-related safeguards, but it is no substitute for the safe and age-appropriate design of digital services, for media literacy, for educational initiatives or for guidance from parents and carers. The aim should therefore be an overall architecture that combines protection, empowerment and digital participation. The practical experience of the digital economy in developing, implementing and applying different methods can make an important contribution to shaping the further legal framework in a way that is effective, privacy-friendly, technology-neutral and workable.

Table of Content

1. What is the purpose of this document? 5
2. About the digital economy 5
3. Terminology – Delineating key terms 5
4. Possible methods 8
5. Data protection aspects 17
6. The EUDI Wallet 18
7. A comparative look at other countries 19
8. Challenges and areas of tension 20
9. Conclusion 21

Technical Paper on Age Assurance

1. What is the purpose of this document?

This document provides a structured, fact-based overview of the terminology, methods, technical operation and areas of application of age assurance. It aims to contribute to an objective assessment of the current political and regulatory debate and to establish a common understanding of the available methods and the conditions under which they operate. The paper expressly takes a technical approach: it neither evaluates individual methods nor derives regulatory preferences, but rather provides a basis for a nuanced, technology-neutral and practice-oriented debate on effective child and youth protection, data protection, technical feasibility and proportionality.

Particularly in an environment in which the debate is often framed as a tension between the objective of effective child and youth protection on the one hand and questions of data protection, technical feasibility and proportionality on the other, the paper creates transparency regarding existing methods, regulatory requirements and current technological developments.

2. About the digital economy

The digital economy is a key driver of innovation, value creation and competitiveness in Germany and Europe. It comprises not only platforms and technology providers, but a broad, interconnected ecosystem of media companies, digital services, games providers, advertisers, agencies, start-ups and data and infrastructure providers. Digital services today shape almost every area of life, including the everyday lives of children and young people – from learning, communication and entertainment to participation in society.

The digital economy therefore bears a particular responsibility for the protection of minors. Many companies in the sector already implement measures that enable age-appropriate services, such as safe default settings, tools for parents and carers or age assurance methods.
Age assurance is a shared task. It involves not only the providers whose services must enforce age limits, but also specialised age assurance providers, identity and trust services, and operating systems and app stores that can provide or pass on age signals. Which solution is appropriate in an individual case depends on the respective service, its risks and its users. The digital economy has extensive practical experience in developing, implementing and applying age assurance methods. This expertise can make an important contribution to a fact-based and practice-oriented political and regulatory debate.

3. Terminology – Delineating key terms

In the policy, academic and business debate on the protection of children and young people online, different terms are used for methods by which the age of users is determined, estimated or verified.

Terms such as Altersverifikation, Altersprüfung, Altersnachweis and Altersfeststellung are frequently used interchangeably in German, although they denote different things. This lack of terminological precision makes it more difficult both to compare technical solutions and to classify them legally and politically.

The paper therefore adopts a uniform terminological framework. Its starting point is the terminology of the Commission proposal for an EU Kids Act (COM(2026) 681 final). The draft uses “age assurance” (German: Altersfeststellung) as the overarching term. It is defined as “a set of methods that can be used to determine, estimate or verify the age of a natural person, including age estimation and age verification and excluding self-declaration by

users" (Article 3(5)(i)). Mere self-declaration by users is thus excluded. The proposal therefore constitutes a key European reference point for the terminology used in this paper. In addition, the paper takes into account a key points paper drawn up jointly in 2024 by the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth (BMFSFJ), the Federal Commissioner for Data Protection and Freedom of Information (BfDI), the Federal Agency for the Protection of Children and Young Persons in the Media (BzKJ), the Federal Network Agency (Bundesnetzagentur) and the North Rhine-Westphalia State Media Authority (Landesanstalt für Medien NRW). That paper uses Altersprüfung ("age check") as the umbrella term for methods by which the age or age range of a person is determined. Within this umbrella term, it distinguishes in particular between age verification and age estimation or age plausibility checks; mere self-reporting of age is likewise excluded. German and European usage are therefore not entirely congruent, but follow a comparable functional logic: a technology-neutral umbrella term covers various methods that differ according to the nature and basis of the age determination. In line with the current Commission proposal, this paper uses "age assurance" as the umbrella term; Altersprüfung is another term commonly used in German. Technical and international frameworks, in particular ISO/IEC 27566-1, are also drawn upon where relevant to a more detailed technical differentiation of the methods. International usage, for example by UK regulators, may be taken into account as a supplement, but is not decisive for the terminological framework underlying this paper.

Within this umbrella term, the paper distinguishes three fundamental methods: age verification, age estimation and age inference. The distinction depends on the information on which an age determination is based and the level of certainty it can achieve.

- **Age verification** establishes with a high degree of certainty, on the basis of identification documents or other sufficiently reliable sources, whether a person has reached a certain age (Article 3(5)(h)). The subject of verification need not necessarily be the exact date of birth. Often it is sufficient to establish that a particular age threshold, for example 16 or 18 years, has or has not been reached.

Age verification is therefore an evidence-based method. Its result is based on a source that already contains reliable information about age or from which compliance with an age threshold can be robustly derived. Depending on the method, this may be, for example, an official identity document, a digital proof of identity or an attestation issued by a trusted entity confirming that an age threshold has been reached.

The German terms Altersverifikation, Altersüberprüfung and Altersnachweis are sometimes used synonymously. In the German original, this paper generally uses Altersüberprüfung (rendered here as "age verification") for the method. By contrast, Altersnachweis ("proof of age") refers rather to the evidence or the result that is used or generated in the course of such a verification.

- **Age estimation** refers to methods that determine a person's age or age range with a certain probability on the basis of specific characteristics. Unlike age verification, the age determination is not based on existing proof of age. The face or behavioural characteristics, for example, may serve as the basis. A well-known example is the algorithmic analysis of a facial image to estimate approximate age. The result is not a definitive determination of exact age, but a probability statement or an assignment to an age range. Age estimation methods must therefore be designed with care, particularly around relevant age thresholds. The closer the estimated age is to a legally or technically defined threshold, the greater the risk of misclassification may be. A system may therefore, among other things, work with safety margins or provide for an additional age assurance method where results are inconclusive. Ofcom expressly distinguishes between age verification and age estimation and, in principle, also permits a combination of the two methods.

- ISO/IEC 27566-1 introduces **age inference** as a third method. This covers methods in which age or the attainment of an age threshold is inferred from existing, reliable information. This may be based, for example, on existing account, contract or other

usage data, provided that these allow a sufficiently robust conclusion to be drawn about age. The age determination is therefore based neither on evidence presented specifically for this purpose nor on direct analysis of the face. Rather, it is derived indirectly from information that is already available in another context. ISO/IEC 27566-1 treats age inference as a method in its own right within the overarching concept of age assurance. The draft EU Kids Act, by contrast, does not explicitly use the term age inference. The paper nevertheless adopts it, as it describes a category of methods that is relevant in practice and allows a clearer distinction from age verification and age estimation. The reliability of age inference depends crucially on the quality and probative value of the source information used.

The methods must be distinguished from the result that is transmitted to a service. The draft refers to this generally as an age signal. As a rule, it does not relate to exact age, but to whether a particular age threshold has been met (Article 3(5)(j)). Such a signal can accordingly indicate both that a relevant age threshold has been reached and that a person falls below it.

The separation between method and result is particularly relevant from a data protection perspective. For an age-related access decision, a service does not need a person's full identity or exact date of birth. Often it is sufficient to know whether the age threshold applicable to the service or content in question has or has not been reached. In addition to the methods, the draft distinguishes solutions according to their regulatory status. EU age verification solutions are certified and listed under an EU-wide procedure (Article 3(5)(k)). The EUDI Wallet is one possible form of such a solution. For certain purposes, the draft also permits other solutions, provided that they meet its requirements (Article 29(4)). With reference to Recital 57, the paper refers to these as alternative age assurance solutions.

The framework chosen in this paper provides a terminological structure for the analysis that follows. It does not imply that all companies, supervisory authorities, legislators and academic institutions use the same terms in the same way.

In German youth media protection, for example, the term age verification system (Altersverifikationssystem, AVS) has become established. It is used in particular in connection with closed user groups under the Interstate Treaty on the Protection of Minors in the Media (Jugendmedienschutz-Staatsvertrag, JMStV). The Commission for the Protection of Minors in the Media (Kommission für Jugendmedienschutz, KJM) understands this to mean systems that combine at least one-off identification to verify that the user is of age with authentication for each individual instance of use. In this regulatory context, the term AVS therefore denotes a particularly specific and stringent form of age control. It is narrower than the umbrella term age assurance used in this paper.

Understandings of the terms also differ internationally. While ISO/IEC 27566-1 categorises age verification, age estimation and age inference under the umbrella term age assurance, Ofcom essentially limits the term in its regulatory application to age verification and age estimation. The ICO, in turn, adopts a broader understanding that, in addition to document-based and biometric methods, also covers self-declaration, technical design measures and tokenised age checks by third parties.

In business practice, the name given to a method is often determined more by its specific function, technical implementation or user interface than by a uniform regulatory framework. Different companies may therefore describe comparable methods differently or use the same term for technically different solutions. In addition, several methods can be combined, for example by first using existing information for age inference and resorting to age estimation or age verification only in cases of doubt.

The interplay of such methods can be illustrated using the Swiss cheese model familiar from safety research. Each method is like a slice of cheese: it catches the majority of cases, but also has holes. In age inference, these arise, for instance, from shared accounts; in age estimation, from imprecision close to the age threshold; and in age verification, from missing

documents or the sharing of login credentials. No single slice is free of gaps. When several slices are stacked one behind the other, however, the holes lie in different places, so that the weaknesses of one method can be offset by the strengths of another.

The effectiveness of age assurance therefore stems less from the perfection of any single method than from their sensible combination. Ofcom, too, concludes that no single method completely rules out circumvention and advocates layered levels of protection.

Which solution is used depends, among other things, on the business model, the risk profile of the service, the user group concerned, the applicable age threshold and the required level of assurance. The name of a method alone therefore does not make it possible to draw firm conclusions about how it works in practice, how reliable it is or whether it is suitable for the regulatory purpose in question.

In the academic and standard-setting debate, too, the focus is increasingly not only on individual technical methods. Rather, complete age assurance systems and their properties are examined, including accuracy, data protection, security, accessibility and acceptance. ISO/IEC 27566-1 likewise follows such a systemic approach and describes a common framework for age-related access decisions without prescribing any single technical method.

4. Possible methods

Age assurance methods are not used solely to implement the EU Kids Act. In Germany, the Interstate Treaty on the Protection of Minors in the Media already requires a closed user group for adults for certain content (Section 4(2) sentence 2 JMStV). Age limits also apply, for example, to gambling or the mail-order delivery of age-restricted goods. At European level, Article 28 of the Digital Services Act (DSA), for example, obliges providers of online platforms accessible to minors to put in place appropriate and proportionate measures. An age signal can work in both directions: it can confirm that an age threshold has been reached, but it can equally show that a person is below that threshold and that certain safeguards must therefore apply, such as the prohibition of profiling-based advertising to minors under Article 28(2) DSA.
The following sections focus primarily on the EU Kids Act, not least because it would, for the first time, systematically regulate age assurance requirements across the Union. However, the methods described are also relevant for the other purposes.

The draft EU Kids Act does not prescribe any particular technical method. Rather, whether a method is permissible depends on the purpose of the obligation in question and on whether it meets certain substantive requirements. This gives rise to two routes:

- For the restriction under Article 6 on minors under the age of 15 independently setting up and using accounts on the social networking and video-sharing services covered by that provision, only a certified EU age verification solution may be used. The restriction applies only where the service concerned poses a risk to the privacy, safety or protection of minors under 15. The solution must rely on an EU proof-of-age attestation provided by a third party whose conformity with the EU age verification framework has been certified and which is included in, or can be verified against, the relevant EU lists (Article 29(2)). Subject to the conditions set out there, Article 6(2) allows limited accounts for minors over 13 and under 15 to be created by a parent or guardian.

- For the inherent-safety obligation under Article 8(1), and for the obligations imposed on app-store providers under Article 16(2) and (3), other age assurance solutions may be used instead of the EU age verification solution referred to in Article 29(2). The provider must demonstrate that those solutions meet the requirements of Articles 27 and 28 (Article 29(4)).

For existing accounts, Article 32 provides for graduated exemptions. Where an account may

belong to a person under 15, a repeat age verification check may be dispensed with if the provider can establish with a high degree of certainty that the user has reached the minimum age laid down in Article 6 (Article 32(1) and (2); Recital 61). Providers subject to Article 8(1) and providers of app stores are not required to determine the user's age if they can establish with a high degree of certainty that the user is not a minor (Article 32(3)). The methods described in this chapter are therefore not permissible or impermissible in the abstract; their suitability depends on the purpose for which they are used and the applicable conditions.

Irrespective of the route chosen, common baseline requirements apply to the methods. They provide the framework for the descriptions below. Article 27 requires a high level of accuracy, reliability, security, robustness, non-intrusiveness, privacy protection and data protection, as well as non-discrimination. Recital 50 elaborates on these criteria: accuracy must be assessed under real-world conditions using publicly available parameters; robustness refers to resistance to circumvention; and non-intrusiveness means that neither a user's identity nor their exact age is disclosed where confirmation that an age threshold has been met is sufficient. Article 28 contains additional data protection requirements. Age assurance solutions must not enable the identification or location of users, tracking, targeted engagement, advertising or profiling (paragraph 1). Providers and entities acting on their behalf must not collect or process more personal data than is strictly necessary to check the relevant age requirement. Further processing, disclosure or linking with additional data, as well as linking with data from other services, is in principle prohibited (paragraph 2). Article 28(3) requires the use of state-of-the-art methods and provides that every age assurance measure must be implemented as a zero-knowledge proof. An age signal may be stored at account level only by the providers expressly identified in Article 28(4) – providers under Article 8(1) and app-store providers under Article 16(4) – and only to avoid repeated age checks; only the minimum information necessary for this purpose may be stored. In addition, a free electronic complaints mechanism must be available for incorrect results (Article 29(5)).

The following overview describes the methods in a structured way according to a uniform framework.

4.1 Age verification

Age verification refers to methods that confirm a person's age on the basis of reliable, verifiable evidence or an authoritative data source. This may include official documents such as identity cards, passports or driving licences, or other reliable sources containing previously verified age data. An identity match may also be required, for example to compare the photograph on a document with the person presenting it. Unlike age estimation, the age determination is based on information that already exists rather than on a statistical estimate; its reliability nevertheless depends on the quality of the source and on whether it has been correctly attributed to the person concerned.

These methods can achieve a high level of certainty and are therefore used above all where a particularly robust level of assurance is required for an age-related decision. At the same time, they entail practical and data protection challenges. For users, they involve greater effort. In addition, personal data from identity documents are processed, unless only an age attribute is transmitted. Providers face technical and legal requirements that become more demanding when users come from different countries with different documents and legal frameworks.

In practice, the following methods in particular are used:

Electronic reading of government-issued documents

Criterion	Description
Attribute assessed	Data stored on the chip of an identity card, passport or residence permit.
How it works	Reading the chip data, for example using the online ID function (eID), and cryptographic verification of authenticity.
Nature of the result	Deterministic.
Classification under the EU Kids Act	For Article 6, only as part of a certified EU age verification solution; alternative solutions only for Article 8(1) and Article 16(2) and (3) (Articles 29(2) and (4)).
Specific features	High level of protection against forgery; requires an eID-enabled document, which younger minors in particular often do not have.
Data protection and data security	May be perceived as intrusive; requires high standards of data security and unlinkability.

Optical document verification with biometric matching

Criterion	Description
Attribute assessed	Identity document and live image of the person.
How it works	Capture of the document and verification of its authenticity features; matching of the photograph against a live image, including liveness detection.
Nature of the result	Deterministic.
Classification under the EU Kids Act	For Article 6, only as part of a certified EU age verification solution; alternative solutions only for Article 8(1) and Article 16(2) and (3) (Articles 29(2) and (4)).
Specific features	Can be used without a chip reader. Robustness against forged or third-party documents depends on document checks, security features and liveness detection. Requires a suitable identity document; the availability and acceptance of such documents may be limited, particularly for minors.
Data protection and data security	Full identity document data and image data may be processed. Data minimisation, immediate deletion after the check and disclosure of only the necessary result to the service are essential. Central storage may give rise to additional security risks.

Video-based or in-person identification

Criterion	Description
Attribute assessed	Identity document.
How it works	Verification of the document by a trained person via video link or in person, for example at a post office.
Nature of the result	Deterministic.
Classification under the EU Kids Act	As for electronic reading; in-person verification is cited as a possible route to the issuance of proof-of-age attestations (Recital 60).
Specific features	Greater organisational and time requirements; suitable mainly for one-off initial enrolment. Requires a suitable identity document; not having a national identity card does not mean that no other form of proof is available.
Data protection and data security	Identity document data are viewed by third parties; video-based methods generate recordings, the retention of which must be limited. Where verification and the service are kept separate, the service learns only the result.

Confirmation by entities holding verified identity data

Criterion	Description
Attribute assessed	Customer data held by credit institutions or other entities subject to statutory identification obligations.
How it works	Confirmation on request that an age threshold has been reached, for example via a banking app or open banking.
Nature of the result	Deterministic, provided that the source presupposes a verified identity.
Classification under the EU Kids Act	For Article 6, only where the third party concerned is certified as a compliant provider of an EU proof-of-age attestation and is included in the relevant EU lists; alternative solutions only for Article 8(1) and Article 16(2) and (3) (Articles 29(2) and (4)).
Specific features	Draws on identities that have already been verified; requires an existing customer relationship.
Data protection and data security	The age determination must be strictly separated from financial data. The confirming entity should not learn for which service the check is being carried out.

Presentation of a digital proof of age

Criterion	Description
Attribute assessed	Previously issued proof-of-age attestation, e.g. in the EU age verification app or the EUDI Wallet ("d-you").
How it works	The credential is stored on the user's device and presented when required; only whether the age threshold has been met is transmitted.
Nature of the result	Deterministic; reuse of the result of a previous initial enrolment.
Classification under the EU Kids Act	As a certified EU age verification solution, also usable for Article 6 (Article 29(3)).
Specific features	No repeat check is required; a suitable device and prior initial enrolment are necessary. Availability depends heavily on the issuance and access requirements of the respective national wallet.
Data protection and data security	With an appropriate protocol and privacy design, the credential can be presented without the service receiving the user's identity or date of birth and without individual uses being linkable. Whether the issuer learns the context of use also depends on the specific technical implementation.

4.2 Age estimation

Age estimation refers to methods that derive a person's age from their face or behavioural characteristics without recourse to proof of identity. The most widespread is the analysis of a live image of the face using trained AI models. Voice, hand geometry or interaction patterns, for example, are also used. Unlike age verification, the age determination is therefore based not on evidence, but on a probability with a certain margin of error. The draft EU Kids Act names age estimation as an age assurance method, but does not define it in further detail (Recital 53).

These methods do not require identity documents and are generally less burdensome for users. They are therefore also accessible to people who do not have a suitable document and are used above all where a relatively simple check is sufficient or where a more stringent method is needed only if the result is unclear. The probabilistic nature of the result nevertheless entails particular requirements. Close to an age threshold, the result is less clear-cut, which is why safety buffers or supplementary checks are used in practice. The KJM has specified fixed safety buffers for certain systems it has assessed: for the "SafePassage Module-Only Solution", a fixed five-year buffer was required for access to 18+ content, meaning that the estimated age had to be at least 23. Other concepts assessed by the KJM provide for different thresholds and fallback checks. It is also necessary to consider whether estimation accuracy varies between different groups of users, which is relevant to the non-discrimination criterion in Article 27. These methods process personal data and, depending on the specific technical design and purpose of processing, may also involve biometric data within the meaning of Article 4(14) GDPR. The input data are therefore particularly important from the perspectives of data minimisation and timely deletion. Under the draft, age estimation cannot replace the certified EU age verification solution required under Article 6. It may be used as an alternative solution for the obligations under Article 8(1) and Article 16(2) and (3), provided that the requirements of Articles 27 and 28 are met (Article 29(4)).

In practice, the following methods in particular are used:

Facial age estimation

Criterion	Description
Attribute assessed	Facial features.
How it works	A trained model estimates age on the basis of a live image.
Nature of the result	Probabilistic; the margin of error is offset by safety buffers.
Classification under the EU Kids Act	Not as a substitute for the EU age verification solution under Article 6; an alternative solution for Article 8(1) and Article 16(2) and (3) only if the requirements of Articles 27 and 28 are met (Article 29(4)).
Specific features	The most widespread estimation method; liveness detection may be required depending on the design. Accuracy and potential differences between user groups must be examined.
Data protection and data security	Personal image data are processed. Whether the processing involves biometric data within the meaning of Article 4(14) GDPR depends on the specific technical processing and on whether it serves the purpose of uniquely identifying a person. Data minimisation, short retention periods or immediate deletion, and – where technically possible – on-device processing are essential. The application of Article 28(3) of the draft requires separate consideration.

Voice-based age estimation

Criterion	Description
Attribute assessed	Voice characteristics.
How it works	A model estimates age on the basis of a short voice recording.
Nature of the result	Probabilistic.
Classification under the EU Kids Act	Not as a substitute for the EU age verification solution under Article 6; an alternative solution for Article 8(1) and Article 16(2) and (3) only if the requirements of Articles 27 and 28 are met (Article 29(4)).
Specific features	Can be used without a camera; accuracy depends on recording conditions.
Data protection and data security	Voice recordings are personal data and may contain additional information. Processing beyond what is

	necessary for age estimation should be avoided; input data should be deleted promptly after the check. Whether biometric data within the meaning of the GDPR are involved depends on the technical processing and its purpose.

Other biometric estimation methods

Criterion	Description
Attribute assessed	Characteristics such as hand geometry.
How it works	A model estimates age on the basis of characteristics that change with age.
Nature of the result	Probabilistic.
Classification under the EU Kids Act	Not as a substitute for the EU age verification solution under Article 6; an alternative solution for Article 8(1) and Article 16(2) and (3) only if the requirements of Articles 27 and 28 are met (Article 29(4)).
Specific features	Less widespread to date; requirements regarding liveness detection and accuracy apply accordingly.
Data protection and data security	Processing hand characteristics may involve personal data and – depending on the technical processing and whether it serves an identification purpose – biometric data. Data minimisation, purpose limitation and short retention periods must be ensured.

Behaviour-, usage- and account-based age estimation

Criterion	Description
Attribute assessed	Interaction and usage patterns, as well as information about users available within the service, e.g. typing or movement behaviour, content consumed or published, and age information in a profile.
How it works	A model estimates a likely age classification or age range from patterns of use and/or user-related information already available.
Nature of the result	Probabilistic for behavioural characteristics (age estimation); indirect for verified information from which age can be inferred (age inference).
Classification under the EU Kids Act	Not as a substitute for the EU age verification solution under Article 6; for Article 8(1) and Article 16(2) and (3), it should be considered as an alternative solution only if

	the requirements of Articles 27 and 28 are met (Article 29(4)).
Specific features	Possible without active user involvement; the boundary with age inference can be fluid.
Data protection and data security	Depending on the specific design, analysis may conflict with the prohibitions on locating, tracking, targeted engagement and profiling under Article 28(1), as well as the restrictions on linking data under paragraph 2. Ongoing or cross-service behavioural profiling should therefore not be treated as an unproblematic form of age assurance.

4.3 Age inference

Age inference refers to methods that use the presence or validity of information already available to infer indirectly whether an age threshold has been reached or not. Sources may include verifiable contract or payment records, verified information from mobile network operators or other reliable contextual information. The information used must genuinely support an inference about the relevant age threshold and be attributable to the user concerned. The mere existence of an account or an email address with a service that has a minimum-age requirement does not, in itself, establish either the age or identity of the current user.

The international standard ISO/IEC 27566-1 treats age inference as an independent method alongside age verification and age estimation. It distinguishes it in particular from estimation based on biological or behavioural characteristics: inference relies on the presence or validity of information from which age can be derived indirectly. Other regulatory approaches, such as Singapore's, sometimes use broader categories that may also encompass account activity or usage data. The draft EU Kids Act does not expressly use the term age inference, but recognises certain existing signals for existing accounts, such as the date the account was created or credit card data lawfully obtained in the past (Recital 61).

These methods draw on data that are already available and therefore generally require no further action from users. They can be used in particular to screen existing accounts with relatively little effort and identify cases in which there is a reliable indication that the minimum age has already been reached. The reliability of the result depends, however, on the quality of the underlying source. Relevant factors include whether a contract actually requires the holder to be an adult and whether the contract holder is the person actually using the service – which may not be the case with family plans or shared payment methods. Where conclusions are drawn from usage behaviour, it must also be assessed whether, under the taxonomy used here, the method still constitutes age inference or is already age estimation based on behavioural characteristics. Ongoing analysis of usage data may also conflict with the prohibition of tracking, targeted engagement and profiling in Article 28(1), as well as the restrictions on linking data in paragraph 2. For very large online platforms, Article 32(4) provides for an implementation plan to be submitted to the competent authority; the probative value of existing age indicators must be explained with suitable evidence and, where appropriate, statistical performance data (Recital 62). Age inference cannot replace the certified EU age verification solution required under Article 6. It may be used as an alternative solution for Article 8(1) and Article 16(2) and (3) only if the requirements of Articles 27 and 28 are met (Article 29(4)).

In practice, the following methods in particular are used:

Payment and contract data

Criterion	Description
Attribute assessed	Contracts that presuppose legal age, e.g. credit cards.
How it works	The existence of the contract is taken as an indication that the holder is of legal age.
Nature of the result	Indirect; meaningful only if the contract actually presupposes legal age (e.g. not a debit card).
Classification under the EU Kids Act	Mentioned as a possible signal for existing accounts in Recital 61; an alternative solution for Article 8(1) and Article 16(2) and (3) only if the requirements of Articles 27 and 28 are met (Article 29(4)).
Specific features	Limited where third-party means of payment are used.
Data protection and data security	Payment data, which are particularly sensitive, are processed. The age determination must be kept separate from other financial information.

Mobile network operator checks

Criterion	Description
Attribute assessed	Account information held by the provider, e.g. the date of account creation.
How it works	The minimum age is inferred from the age of the account or from existing account information.
Nature of the result	Indirect.
Classification under the EU Kids Act	Possible as an alternative solution for Article 8(1) and Article 16(2) and (3), provided that the requirements of Articles 27 and 28 are met (Article 29(4)).
Specific features	No additional data collection; limited in the case of shared accounts.
Data protection and data security	Only data that are already available are used. Where usage data are analysed, the distinction from impermissible profiling (Article 28(1)) must be observed.

Account and usage data

Criterion	Description

Attribute assessed	Account information held by the provider, e.g. the date the account was created.
How it works	The minimum age is inferred from the age of the account or from account information already available.
Nature of the result	Indirect.
Classification under the EU Kids Act	The date an account was created is mentioned as a possible signal for existing accounts in Recital 61; requirements for handling such signals and the implementation planning of very large online platforms arise in particular from Article 32(4) and the relevant recitals.
Specific features	No additional data collection; limited in the case of shared accounts.
Data protection and data security	Only data that are already available are used. Where usage data are analysed, the distinction from impermissible profiling under Article 28(1) must be observed.

E-Mail-based inference

Criterion	Description
Attribute assessed	Usage history of an email address.
How it works	Age is inferred from the use of the address for services that require a minimum age.
Nature of the result	Indirect.
Classification under the EU Kids Act	Possible as an alternative solution for Article 8(1) and Article 16(2) and (3), provided that the requirements of Articles 27 and 28 are met (Article 29(4)).
Specific features	Possible without user involvement; depends on the quality of the underlying data sources.
Data protection and data security	The check draws on third-party data; data minimisation and the prohibition on linking data under Article 28(2) must be observed.

5. Data protection aspects

Age assurance methods are subject to an inherent tension. They are intended to protect minors, but may require the processing of data relating to all users in order to do so. The distinction between age assurance and identification is central here. For an age-related access decision, a service generally does not need to know who a person is, but only whether they have reached a certain age threshold.

The Commission proposal for an EU Kids Act takes up this idea with requirements that go beyond the general principles of the GDPR. Under Article 28(1), age assurance solutions must not enable the identification or location of users, tracking, targeted engagement,

advertising or profiling. Under Article 28(2), providers and entities acting on their behalf must not collect, store or process more personal data than is strictly necessary to check the relevant age requirement. Further processing, disclosure or linking with additional data, as well as linking with data from other services operated by the same provider or by third parties, is in principle prohibited. The GDPR remains applicable alongside these requirements. The data protection supervisory authorities are responsible for monitoring compliance with the data protection obligations under Articles 27, 28 and 29 (Article 34(6)).Three key architectural principles can be derived from these requirements:

- The first principle is **data minimisation** at the level of the result: ideally, the service receives not the date of birth but only an indication of whether the relevant age threshold has been met. The extent to which this can be achieved depends on the method. It is inherent in attestation-based methods. With other methods, the checking service provider may initially receive additional data, such as full identity document details or a facial image, which should generally be deleted promptly after the check, unless another legal basis permits limited retention. From a data minimisation perspective, the exact age should not be stored permanently; where storage is lawful, only whether the relevant condition for use has been met should be retained. Two levels must be distinguished: a digital proof of age is held on the user's device, for example in an app or wallet. Under Article 28(4) of the draft, however, an age signal may be stored at account level only by the providers specified there (providers under Article 8(1) and app-store providers under Article 16(4)). Such storage may be used solely to avoid repeated age checks and must be limited to the information strictly necessary for that purpose.
- The second principle is the **separation of roles**. The entity that verifies age should not learn for which service the check is being carried out, and the service should not learn who the person is. France has made this principle mandatory as "double anonymat" (double anonymity). The Commission describes its own solution as "double-blind", untraceable and unlinkable.
- The third principle is the **zero-knowledge proof**: a cryptographic method that makes it possible to prove the validity of a statement without disclosing the underlying data. The EU reference solution for proof of age uses corresponding cryptographic methods; some of the technical components and implementations are documented as open source. Article 28(3) of the Commission proposal requires the use of state-of-the-art methods and provides that every age assurance measure must be designed as a zero-knowledge proof.

These principles cannot be implemented technically in the same way for all methods. In attestation-based age verification, a cryptographic proof of an age attribute that has already been confirmed is a particularly straightforward approach. Age estimation, by contrast, generates its result only after analysing biological or behavioural characteristics; it does not necessarily rely on a previously signed age attribute. For age inference, feasibility depends on whether the underlying information is available as verified, cryptographically verifiable evidence. The model used in the reference solution therefore cannot readily be transferred to estimation or non-attestation-based inference methods. However, zero-knowledge methods are not inherently limited to signed proof-of-age attestations: cryptographic proofs that a model calculation has been performed correctly are also conceivable. Such approaches are technically demanding and should be distinguished from the straightforward verification of a signed attribute. Regardless of the specific implementation, input data should be processed locally wherever possible, minimised and deleted promptly, with only the necessary result being disclosed. Further technical clarification is needed on how Article 28(3) is to apply to the different methods.

6. The EUDI Wallet

The European Digital Identity Wallet (EUDI Wallet) is based on the revised eIDAS Regulation. Member States must make at least one EUDI Wallet available in accordance with the eIDAS Regulation; the relevant implementing acts set the deadline for doing so at the end of 2026.

Germany's state wallet "d-you" is scheduled to launch in early January 2027 and will be available free of charge and on a voluntary basis to citizens and residents of Germany. The wallet allows identity data and other credentials to be stored on a suitable device and individual attributes to be presented selectively, for example only the statement "over 18". Verified age attributes can be provided by qualified trust service providers in the form of qualified electronic attestations of attributes (QEAAs). Depending on the design, public authorities or other entities holding reliably verified information may also serve as underlying data sources. Open standards such as ISO/IEC 18013-5 (mDoc), OpenID for Verifiable Presentations (OpenID4VP) and the W3C Digital Credentials API are intended to support the interoperability of such credentials across national, platform and provider boundaries. They do not, by themselves, guarantee access through all browser and app environments; the specific implementation and support provided by the systems involved are also decisive. Until wallets are widely available, the Commission is testing an interoperable reference solution through its EU age verification Blueprint, which is being piloted in several Member States in 2026. Under the EU Kids Act, a wallet that meets the requirements of the EU age verification framework is deemed to be a certified EU age verification solution (Article 29(3)). It thus occupies a special position in the draft's regulatory model, but it is not the only possible form of age assurance. Particularly during the transition phase, other methods are also available, such as banking identities, payment data or estimation methods. This means that people without a wallet can also prove their age.

7. A comparative look at other countries

Regulation of age assurance is also being advanced outside the European Union. The terminology largely corresponds to the framework used here. However, the regulatory approaches differ in terms of where they intervene and how much latitude they give providers in choosing a method.

Under the Online Safety Act, the United Kingdom requires "highly effective age assurance". A method must be technically accurate, robust, reliable and fair. Ofcom, the regulator, provides a non-exhaustive list of suitable methods: open banking, photo-ID matching, facial age estimation, mobile network operator checks, credit card checks, digital identity services and email-based age estimation. Self-declaration is expressly regarded as insufficient. Ofcom emphasises that no single method can prevent all attempts at circumvention and therefore recommends selecting appropriate measures according to the level of risk. The UK Government also plans to restrict access to certain social media services for under-16s, following the Australian model. The first implementing rules are expected to be published by the end of 2026, with the measures scheduled for implementation in spring 2027.

Australia was the first country to pass a statutory minimum age of 16 for the use of certain social networking services at the end of 2024. The law entered into force on 10 December 2025. Providers must take "reasonable steps" to prevent people under 16 from holding accounts on the services covered by the law. The obligation rests with the platforms, not with children or their parents. Providers have considerable latitude in choosing the method. The Australian data protection authority expressly distinguishes between age verification, age estimation and age inference.

Other countries place greater emphasis on age assurance at the app-store or operating-system level. In Singapore, app distribution services designated by the competent regulator have been required since 31 March 2026 to implement age assurance measures to prevent users under 18 from accessing apps whose age ratings are not appropriate for them. These services may choose between age verification, age estimation and age inference, or a combination of these methods. In the United States, several states have enacted or proposed rules on age categorisation at app-store level, although their start dates and legal status vary. California's Digital Age Assurance Act relies on an age signal from the operating system, which is to be made available gradually from 1 January 2027. Brazil's Digital Statute for Children and Adolescents (ECA Digital, Law No. 15,211/2025), in force since 17 March 2026, covers digital products and services directed at or capable of being used by children and young people. For access to products or services prohibited by law, a mere self-

declaration of age is insufficient.

The comparison shows that similar methods are embedded in different regulatory approaches. The United Kingdom focuses on the effectiveness of methods, Australia relies on an open-ended "reasonable steps" standard, and other countries shift certain obligations to app stores and operating systems. The draft EU Kids Act, by contrast, differentiates according to the regulatory status of the solution. In the approaches considered here, self-declaration alone is often insufficient, but the scope and specific design of the requirements vary considerably.

8. Challenges and areas of tension

The preceding chapters show that age assurance is not merely a technical side issue. It can be an important prerequisite for age-related safeguards in the digital environment where those safeguards depend on the actual age of the user. Age limits, age-appropriate default settings and feature restrictions may require reliable age information, but they do not in every case require a separate age assurance check. Age assurance should therefore be understood as a possible component of digital protection infrastructure, not as a blanket condition of access to all digital services. Such protective infrastructures may also include mechanisms involving parental support. Where appropriate for the relevant use case and required by regulation, technical solutions should therefore also provide for the involvement of parents or legal guardians.

Age assurance also concerns people other than children and young people. To identify minors reliably, adults must also prove their age. The ability to use lawful information and services anonymously or pseudonymously is an essential feature of a free internet and is closely linked to freedom of expression and information. The challenge is therefore to reconcile effective child protection with data protection, open access to digital services and the fundamental freedoms of users.

No method meets all requirements equally. The methods differ in terms of accuracy, reliability, robustness, data protection, effort and accessibility; at the same time, no single method can completely rule out circumvention. Which method is appropriate and what level of assurance is required should therefore depend on the specific risk posed by a service, item of content or feature. Higher risks may justify more stringent requirements, while lower-risk services should not automatically be subject to the same depth of checking.

This balancing exercise must also take into account how many and which users are affected by a check. Age assurance can be used in a targeted way for access to specific content or features. However, it can also be designed as a general condition of access, thereby covering large parts of the population, including adults with no need for protection under youth protection law. The larger the group of people affected and the broader the effect on access, the more demanding the requirements in terms of proportionality, data minimisation, accessibility and usability.

Such an approach therefore starts primarily from the required outcome: an appropriate level of assurance must be achieved for a specific use case. This makes it possible to deploy different technical solutions according to the respective need for protection, without requiring a uniform method for all use cases. Age assurance can accordingly be applied in a targeted way where a specific risk exists, for example in live streaming, direct messages with strangers, in-app purchases or access to 18+ content. Tiered and combined methods, as also provided for in the international standard ISO/IEC 27566-1, reflect this idea.

Regulatory requirements should therefore be formulated in a technology-neutral way and be guided by verifiable quality and effectiveness requirements. Permanently locking in individual methods can quickly become outdated in view of technical developments and may limit innovation. However, technology neutrality requires sufficiently specific benchmarks so that providers can reliably assess which solutions meet the regulatory requirements. User trust is equally important. Methods that lack transparency or are perceived as excessively intrusive can encourage acceptance problems and evasive behaviour, thereby reducing their protective effect.

Age assurance is, moreover, a task for the entire digital ecosystem. Operating systems, app stores, identity services, platforms and public authorities each bear their own responsibility. These responsibilities must be clearly allocated. Operating systems and app stores can provide age signals, but service providers are best placed to understand the risks of their own services and features. Shifting responsibility unilaterally to a single level would not do justice to this. Public identity infrastructures such as the EUDI Wallet are an important building block, but do not relieve stakeholders of the task of ensuring accessibility for all – in particular for children and young people without identity documents, for people without suitable devices and for people with disabilities. The parallel availability of several methods is therefore also a requirement of digital inclusion.

As digital services are offered across borders, European harmonisation is preferable to a multitude of individual national solutions. Divergent requirements increase implementation costs, create legal uncertainty and lead to an inconsistent level of protection. Mutual recognition of credentials and compatibility with international standards are essential in this respect. Legal certainty is also a prerequisite for investment. As long as it remains unclear which methods are considered compliant, implementation will be delayed and providers with greater resources will be favoured. The requirements must therefore also be workable for small and medium-sized enterprises.

Finally, age assurance is necessary but not sufficient. It enables safeguards, but it is no substitute for the safe design of services, media literacy, guidance from parents and carers or educational initiatives. Its effectiveness should also be evaluated regularly so that regulatory requirements are evidence-based and can be adapted to technical and societal developments.

9. Conclusion

Age assurance has become a key element of the protection of children and young people online. This paper shows that there is no single solution, but rather a broad spectrum of age verification, age estimation and age inference methods. These methods differ in their level of certainty, the effort involved and their impact on data protection. Their effectiveness therefore depends less on any single technique than on how they are selected, combined and designed.

This points first to the need for a risk-based, tiered approach. A uniform solution for all services would reflect neither the differences in risk nor users' differing needs. Instead, a tiered sequence of measures should be used, with the strength of the age determination matched to the level of risk associated with the service or feature.

Secondly, data protection and data security must be built into the technology from the outset. Methods that transmit only the required age attribute, prevent uses across different services from being linked and rely on zero-knowledge proofs demonstrate that effective protection and privacy are compatible. Storing copies of identity documents or other sensitive data on central servers, by contrast, should be avoided, as it creates new security risks and undermines user trust.

Thirdly, open and interoperable interfaces are needed. Standards and specifications such as the W3C Digital Credentials API, ISO/IEC 18013-5 and OpenID4VP can make it easier to integrate wallets and credentials from different providers across different operating systems and provider environments. They can reduce technical dependencies and promote competition and innovation. This depends, however, on the standards being implemented interoperably and actually supported by the systems involved.

Fourthly, the European Single Market must be protected. Digital services are offered across borders. Fragmented national approaches to youth protection can lead to legal fragmentation, higher costs and an inconsistent level of protection. The Digital Services Act already provides a common European framework for the protection of minors on online platforms. It should be applied coherently and complemented, without creating contradictions, by new Union-wide requirements, particularly those concerning age assurance.

Finally, a genuine balance must be struck between protection, empowerment and participation. Youth protection must not result in children and young people being excluded from digital services that are important for education, communication and participation in society. Technical age assurance is therefore only one building block. It must go hand in hand with the age-appropriate design of services, the promotion of media literacy and guidance from parents and carers.

The digital economy has extensive experience with the methods described here. It stands ready to contribute this expertise to the further development of the legal framework so that age assurance is effective, privacy-friendly and workable.

German Association for the Digital Economy (BVDW)

The German Association for the Digital Economy (BVDW) represents the interests of companies that operate digital business models or whose value creation is based on the use of digital technologies. With members from across the entire digital economy, the BVDW is already shaping the future today – through creative solutions and state-of-the-art technologies. As a catalyst, guide and accelerator of digital business models, the association is committed to fair and clear rules and advocates an innovation-friendly framework. In doing so, the BVDW always keeps the economy, society and the environment in view. In addition to DMEXCO, the leading trade fair for digital marketing and technology, and the Deutscher Digital Award, the BVDW also hosts the CDR Award, the first award in the DACH region for corporate digital responsibility and digital sustainability, as well as a wide range of specialist events.

How this paper was developed

This paper is the result of a joint working process involving several BVDW working groups. Experts from member companies contributed their perspectives. The paper thus brings together the views of those who implement age limits in their services.

The work was based on the practical experience of the participating companies in developing, implementing and applying age assurance methods. This practical perspective was combined with an analysis of the current legal framework, in particular the Digital Services Act and the Commission proposal for the EU Kids Act, as well as international standards and regulatory approaches. The aim was to create a common understanding of the available methods and to enrich the debate with a well-founded, technology-neutral perspective from the digital economy. The paper reflects the joint view of the participating working groups and not necessarily the position of each individual member company.

Contact: **Fabian Miller**, Junior Public Affairs Manager – Data Society, miller@bvdw.org

www.bvdw.org

Imprint

Place and date of publication: Berlin, 15 November 2026

Publisher: Bundesverband Digitale Wirtschaft (BVDW) e. V., Obentrautstraße 55, 10963 Berlin, +49 30 2062186 - 0, info@bvdw.org, www.bvdw.org

Executive Board pursuant to Section 26 BGB (German Civil Code): Carsten Rasner

President: Dirk Freytag

Vice Presidents: Thomas Duhr, Anke Herbener, Corinna Hohenleitner, Dr Moritz Holzgraefe, Björn Kaspring, Julian Simons

Contact: politik@bvdw.org

Register of associations number: Charlottenburg Local Court (Amtsgericht Charlottenburg), VR 42449 B

Legal notice: All details and information contained in this publication have been carefully researched and checked by the Bundesverband Digitale Wirtschaft (BVDW) e. V. This information is provided as a service by the association. Neither the Bundesverband Digitale Wirtschaft (BVDW) e. V. nor the companies involved in the preparation and publication of this work can accept liability for its accuracy, completeness or timeliness. The contents of this publication and/or references to third-party content are protected by copyright. Any reproduction of information or data, in particular the use of texts, parts of texts, images or other content, requires the prior consent of the Bundesverband Digitale Wirtschaft (BVDW) e. V. or the rights holders (third parties).

EU Transparency Register number: 479540331468-69 · German Lobby Register: R000257