Your response

Question	Your response
Question 1: Do you agree with our proposed guidance on scope? If not, please provide any information or evidence in support of your views, including descriptions of services or content where you consider it is unclear whether they fall within the scope of Part 5.	Confidential? – Y / N We agree with the proposed guidance on scope, however, we would like to comment on what is stated in section 2.14 on exclusions. Here it is stated that paid advertising and content appearing in search engine search results are types of pornography excluded from the application of this guidance. We believe that in many instances it is difficult or even impossible to disaggregate commercial or advertising communications from other, more harmful content on video service platforms, and that the approach of establishing age-verification mechanisms for all content, further limiting such cases of exceptions, makes sense. It is crucial to recognise that advertising and search results may also contain harmful content that should be equally protected from access by minors. The presence of such content in advertising space and search results amplifies the need for safety and age verification measures to safeguard younger users from potential risks and unwanted exposure. Related to the above, one reflection being made is that perhaps not all services or platforms require the same age control model. Therefore, one must consider the availability of video thumbnails, content descriptions, or search suggestions, which may already fall under the classification of potentially harmful content, implying that it may be more suitable or straightforward in some cases to protect the website as a whole (and the contents shown in search engines) rather than specific content. For instance, it would be reasonable for a social network to require age verification to access videos with potentially violent content, but not impose restrictions for accessing music or crafting videos. The same would apply to movie and series platforms, where their classification could be leveraged to request age verification or not. However, on a website with pornographic content, it could be understood that all its content should be protected with an age verification system.
Question 2: Do you have any comments on how our proposed guidance applies in respect of pornographic content created by generative-AI services	Confidential? – Y / N We appreciate your query regarding the proposed guidance and its application in relation to pornographic content generated by AI services within the scope of Part 5. We recognise that, as technology providers, our expertise may not be specifically tailored

Question	Your response
within the scope of Part 5? Please provide any information or evidence in support of your views.	to address this nuanced aspect and we may not be best qualified to answer this question comprehensively. However, we are open to further discussions. We would be happy to arrange a meeting to discuss this issue further and to discuss any other matters.
Question 3: Do you have any comments on our proposed guidance in respect of the kinds of age assurance which could be highly effective? If you consider there are other kinds of age assurance which have not been listed that you consider could fulfil the proposed criteria, please identify these with any supporting information or evidence.	Confidential? – Y / N OFCOM has only considered the facial age estimation method in the study, as it is noted that there is no evidence to suggest that other age estimation methods may currently be very effective, are sufficiently mature technologies or are being implemented on a large scale. We agree with the proposed method. Anyway, we would like to suggest that regulation and criteria issued by OFCOM on age verification systems should aim for technological neutrality, as far as possible, or at least leave the door open to other options that pose the same or equivalent degree of security. In this way, minimum requirements to be met by solutions, examples, etc. can be provided, which would be useful for providers and other actors involved. If, on the other hand, OFCOM chooses to list in great detail the solutions that can be used or lists them as a *numerus clausus*, there is a risk of leaving out other mechanisms that now or in the future (it is essential to take into account the rapid technological progress in this area) could be useful and equally valid for the objective pursued. It should also be borne in mind that the users of the platforms of these content providers can be very diverse, and offering them different options to prove their age can be very positive for them to choose the one or ones that best suit their interests: ease of use, convenience, user experience, security... In this way, we consider it appropriate that each provider should be free to decide on the age verification mechanisms to be implemented, as long as they comply with the minimum requirements established by OFCOM, and that users should be free to choose the one or ones they consider most convenient. We would like to take the opportunity of answering this question to propose to OFCOM other solutions that can guarantee the accuracy and precision in identifying and specifying the age of the access applicant. They would imply the processing of more data, but it can be the appropriate solution in some complex cases or even as a second step in the solution initially proposed by OFCOM.

Question	Your response
	1. **Age verification using an identity document and a selfie photograph.** This solution entails requesting the user to provide a capture of their identity document along with a selfie photograph. It is akin to the process employed in sectors such as banking, insurance, mobility, telecommunications, etc. The automatic reading of the identity document is performed to extract the date of birth, thereby facilitating the straightforward calculation of the user's current age. This method of identification also allows for the retrieval of other personal information when necessary, such as the user's name, surname, and ID number. Thus, this solution may be suitable in scenarios where a comprehensive identity verification process is conducted (known in certain contexts as KYC or Know-Your-Customer). These solutions should incorporate technology to validate the authenticity of the identity document. Otherwise, a user could potentially use a fake or altered identity document with a different date of birth. Additionally, the solution should require the capture of a selfie photograph with proof of life to enable biometric comparison between the photograph printed on the identity document and the selfie. This ensures that the bearer of the identity document is indeed its legitimate holder, preventing situations where a minor may use, for example, the identity document of a parent or legal guardian. In the realm of facial biometrics, the National Institute of Standards and Technology (NIST), under the United States Department of Commerce, evaluates the quality of biometric engines globally. According to the NIST FRTE 1:1 report dated November 21, 2023, 150 biometric systems exhibit a false positive rate of 0.000001 and a false negative rate of less than 0.005, measured in the VISA category. This means that the accuracy reaches 99.9999% when comparing faces of different individuals, while only rejecting 0.5% of cases where faces of the same individual are compared, and the individual is attempting recognition by the system. Regarding the capability to perform liveness detection to prevent attackers from impersonating users, there are international standards in place for regulation. Specifically, ISO 30107 establishes the different types of presentation attacks that must be detected. In practice, leading biometric solutions in the market hold iBeta

Question	Your response
	Level 1 and Level 2 certifications according to ISO 30107, ensuring secure use of certified biometric technologies. Moreover, as mentioned, this process can be used as a second step in those scenarios where the age estimation system based on a facial photograph provides inconclusive results. **2. Age verification for successive service accesses (authentication).** The aforementioned process allows for verifying the user's age through a complete identity verification process. However, it is essential to ensure that the user accessing the service in subsequent accesses is of legal age, through successive authentication processes. The use of passwords and devices assumes that the user authenticating through these means is who they claim to be. However, these mechanisms do not guarantee with certainty whether the authorised user is indeed accessing the service or content. For instance, a password can be stolen or simply guessed through social engineering. Therefore, it must be considered that the use of passwords does not ensure with certainty that the person accessing the service is indeed of legal age. This is a known risk and, in some cases, an assumed one, but it is also advisable to evaluate it in defining the requirements of age verification systems. According to a report published by Google, 65% of people use the same password across all or most of the services they use. Additionally, the use of some passwords is common. For example, NordPass published the 200 most common passwords worldwide, with the password "123456" being used by more than four and a half million people. When a password is compromised, it can be exposed and put up for sale on the dark web. According to a report published in 2020 by Digital Shadows, over 15 billion passwords were published on the dark web, with an average price of $15. Therefore, in cases where passwords are used as an authentication element in successive accesses, it is essential to consider the security measures that these passwords must meet, in terms of strength, renewal, custody, etc. On the other hand, to mitigate this risk, some other sectors resort to the use of biometric technologies since authentication with these technologies relies on the user performing the process rather than on user keys or passwords. In the case of accessing the service

Question	Your response
	or content, it would involve basing authentication on verifying that the accessing person is the one previously verified, and thus, of legal age. The use of these biometric technologies for access involves requesting a selfie photograph from the user at the time of access and subsequently performing biometric comparison against the data from the registration process (described in the previous section). This new biometric capture must feature liveness detection technologies that prevent user impersonation, similar to those described earlier. Finally, as a result of the registration process described or a similar one, authentication can be carried out through the sharing of age attributes, under a proposal similar to that introduced by the European eIDAS Regulation with the digital identity wallet. In this regard, the authentication process is simplified at the time of authentication, although it would be necessary to ensure that only the registered user has access to that wallet or app from which to share their attribute.
Question 4: Do you agree that service providers should use the proposed criteria to determine whether the age assurance they implement which is highly effective at correctly determining whether or not a user is a child? Please provide any information or evidence in support of your views.	Confidential? – Y / N Veridas agrees with the criteria: technical accuracy, Robustness, Reliability and Fairness and supports OFCOM's decision to rely on the research of the Age Verification Certification System (ACCS) on the measurement of age verification technologies to develop the proposed list of parameters. However, we would like to see this guidance go a step further and even mention in detail the possibility of establishing audits and certifications to ensure compliance with age verification requirements. In this respect, audits and certifications should be conducted on the obligated entities, in this case, the service providers. However, it is proposed that different providers of age verification solutions may certify their solutions with the relevant authority, based on reports issued by independent conformity assessment laboratories. It is considered that defining the guarantees to verify users' age should not be dependent on the type of solution or technology proposed. Conversely, it is believed that the necessary standards should be established to achieve the goal of preventing minors from accessing harmful content, thereby allowing technologies to adapt to meet the established standards. Similar to other security certifications, there is a proposal to define a set of test scenarios where the solution to be certified demonstrates its ability to grant access to adults and prevent

Question	Your response
	access by minors. In this regard, the following criteria are suggested for defining the tests: A significant number of access attempts by adults and minors (for example, around 1,000 tests). On other occasions, a time limit is established for the tests (for example, 1 week). First access tests (equivalent to registration when necessary), as well as successive accesses to the service (equivalent to an authentication process). Tests in scenarios of collaborative impersonation attempts (e.g., sharing of keys) and non-collaborative impersonation. Establishment of certification criteria for both processes that simulate adult access and those cases that simulate minor access. For example, one criterion may be to certify a 0% access rate by minors, while the access rate by adults exceeds 90%.
Question 5: Do you have any information or evidence on the extent of circumvention risk affecting different age assurance methods and/or on any steps that providers might take to manage different circumvention risks for different methods?	Confidential? – Y / N It is true that certain forms of age assurance and biometric technology in general can carry risks; however, it is essential to note that the state of the art allows developers and companies to mitigate the majority of these risks: **1.** Quality and non-discrimination in biometric technology have made significant progress in recent years. Evaluations conducted by international bodies such as the National Institute of Standards and Technology (NIST) play a crucial role in this advancement. NIST carries out comprehensive testing and assessment of various biometric systems, establishing benchmarks and standards for accuracy and fairness. Current evaluations, standards, and certifications have been pivotal in ensuring the advancement of biometric technology. The technology has now (in fact, there are studies in this sense since 2014) surpassed human capabilities in terms of precision and exhibits fewer biases, which if any are quantifiable in opposition to human bias. This signifies a substantial leap forward in the reliability and equity of biometric technology. Anyway, regarding the bias that is commonly attributed to biometric systems, the focus must be placed in developing, training and testing phases, where the potential issues of the system may be originated at. Should these phases have been appropriately designed and managed, biometry has proven to ensure a better level of equality, non-discrimination and reliability than

Question	Your response
	human-based analysis. Standards and guidelines in this regard could be helpful, and it shall also be taken into account the availability of databases and the capacity to create them by developers, making collaboration by state agencies and developers in these phases highly desirable. **2.** The concept of 'Privacy by Design and by Default' is of paramount importance in the context of reducing risks associated with biometric technologies. It entails the incorporation of robust privacy measures throughout the development and implementation of biometric systems. This approach dispels prevalent myths and misconceptions, ensuring user data remains secure. It could be said that the key element in a biometric recognition system is the engine to be used. Logically, from a technical perspective, more advanced engines naturally offer greater precision, reliability, and improved system accuracy. However, this choice is also critical in ensuring data protection and user privacy. Cutting-edge biometric technologies, which are now the "state of the art", are AI-based and therefore have some inherent characteristics that significantly enhance privacy and security. To shed light on this, we can categorise biometric engine models into two types: ● **Biometric models based on landmarks or "Old-school" models** "Old-school" biometric engines were the most widespread until around 7 to 10 years ago, and are based on 'landmarks' or distinctive points to identify features, for instance, when recognizing a person's face. This method entails measuring various points on the biometric characteristic, such as a facial image, resulting in a mathematical vector that summarises these measurements. This is where the name bio-metrics comes from. However, this type of model may carry data protection risks, since an individual with sufficient knowledge of the system might, based on the vector generated by this biometric engine, interpret the measurements this vector is representing of the distinctive points of the subject's face (e.g. facial image: the distance between the eyes, ears, etc.) to obtain an estimation of the original image. Therefore, with this information, it might be possible to reconstruct the original image and identify the subject. Additionally, these systems were mostly standardised, which means that anyone can learn how to use them (the standards are public

Question	Your response
	through organisations such as NIST). While standardisation promotes interoperability (as seen in fingerprint recognition systems), it also raises significant data protection concerns. ● **Biometric models based on Artificial Intelligence** Leading technology companies developing state-of-the-art systems have transitioned from "old-school" models to those based on Artificial Intelligence and, particularly neural networks. In this model, the generation of the mathematical vector is more complex than simply measuring the subject's biometric distinctive points. Here, the resulting mathematical vector is dependent on the Artificial Intelligence within the biometric engine (though the system may incorporate other mathematical variables, the core components are Artificial Intelligence algorithms). Consequently, when, for example, a facial image is processed through two different biometric engines (or even two different versions of the same engine), the resulting vectors will be entirely different. As a result, in the Artificial Intelligence-based model, even the expert engineer who designed the system cannot interpret the mathematical vector to extract information from the individual who provided their data. Therefore, having the vector does not allow for the extraction of information about the individual it belongs to or their identification. Possessing such a vector does not compromise the identity of the individual. So, it is evident that the implications for the privacy and data protection of biometric data steam from the utilisation of an AI-based biometric engine. Going back to the "privacy by design and by default", the following inherent characteristics can be said regarding this resulting biometric data: - **Irreversibility:** the biometric vectors resulting from AI-based biometric models cannot be reversed to obtain the original raw data used (e.g. the exact facial image of the individual) to create this vector. In this regard, the vector is irreversible and private, which, simplifying, could be assimilated to a hash. - **Non-interoperability:** interoperability between different systems is one of the most common concerns. Nevertheless, if it was explained before that from the same original data each version of a biometric engine created a different vector, the same would be true the other way around: each vector can only be interpreted by the exact version of the biometric engine that created it. While this

Question	Your response
	may sometimes be inconvenient from a technological point of view, it is beneficial from a data protection perspective. - **Temporality**: in any case, it is worth mentioning that a vector is only a representation of the subject's biometric characteristic for the purpose of comparison (in a specific biometric engine), and that it does not provide any further information about the subject. Other purposes (categorisation, emotion recognition,...) may need the same raw data (e.g. a facial image) but that is a different technology/system with a different purpose. - **Controlled use**: as a consequence of the above, the modern biometric vectors are data with limited usability, and they can only be effectively utilised by the individual to whom it belongs. Even in the event of potential theft, the impact on the user is minimal. The vector alone does not grant access to any system. For recognition purposes, at least two pieces of biometric data are employed for comparison, with one usually captured simultaneously (the second can be a vector if there has been a previous registration, or another piece of data captured at that moment when there is no registration). Moreover, users can only employ their vector in systems equipped with a specific biometric engine (the one used for its creation). To further enhance security, signature and encryption techniques are typically applied if the vector is delivered to the subject. This approach would ensure that even systems employing the same engine but implemented by different entities or for different purposes remain non-interoperable. - **Renewal:** it is quite common to hear that biometric data is immutable and that in case it is compromised, the greatest risk is that it cannot be changed as one would do with a password, for example. However, this is not entirely accurate. While a person's face will certainly remain the same, the interpretation of their facial features carried out by a biometric recognition system can indeed be changed. This is made possible by what was explained earlier regarding the intrinsic dependency on the version of the biometric engine used to generate a vector: a new version of this engine will produce a completely different biometric vector from the one created by the old version (even if the same facial image is used), and these two vectors will not be interoperable with each other. Therefore, knowing that

Question	Your response
	creating a new version of the engine is as simple as making slight modifications to certain variables, we find that renewing vectors in case of compromise is just as straightforward as changing passwords. - **Specific use**: although some details of the characteristics mentioned above may be more related to scenarios where biometrics are used for the purpose of recognizing or identifying a person, it must be noted that this purpose is different from that of estimating the age of a person (these systems are often considered as "biometric classification"). Therefore, in addition to what has been explained regarding the privacy of the vector itself, it should be emphasised that these are different technologies, so in terms of data protection, they serve differentiated purposes, as they do not involve the same data processing or even the same technology. The ICO has recognized this differentiation. In conclusion, 'Privacy by Design and by Default' that can be attributed to AI-based biometric models is instrumental in dispelling myths surrounding biometric technology. It safeguards user privacy by reducing the impact of data breaches, reinforcing the concept that, in practice, biometric data remains highly secure and specific to the rightful owner, further solidifying trust in biometric systems. To try to make this idea better understood, we have come up with the following video, in which during minutes 1:15 and 1:45 we explain how this vector generation works https://youtu.be/UWAAwOKs0_g?t=75. On the other hand, referring to specific strengths and weaknesses related to different age assurance methods, please see **Annex I** below where we have included a table with a more complex analysis.
Question 6: Do you agree with our proposed guidance that providers should consider accessibility and interoperability when implementing age assurance? Please provide any information or	Confidential? – Y / N Absolutely, we concur with the proposed approach outlined in your guidance regarding the incorporation of accessibility and interoperability considerations in age assurance implementation. It's essential for service providers to embrace these principles to ensure that age verification processes are not only user-friendly but also effective for all individuals. The principle of accessibility underscores the importance of age assurance methods being straightforward to use and accessible to a diverse range of users. This entails not only offering a variety of age

Question	Your response
evidence in support of your views.	verification methods but also designing user experiences that cater to different abilities and preferences. By doing so, service providers can mitigate the risk of excluding certain demographics and ensure equitable access to legal content. Similarly, interoperability plays a pivotal role in enhancing the efficiency and effectiveness of age verification processes. It involves enabling seamless communication between different technological systems through standardised formats and protocols. By fostering interoperability, service providers can streamline age verification procedures and potentially reuse verification results across various platforms, thereby enhancing user experiences and compliance with regulatory requirements. While we acknowledge the current absence of operational infrastructure and standards facilitating interoperability between age assurance providers, we commend the proactive approach outlined in the guidance to monitor and evaluate developments in this area. This forward-thinking approach demonstrates a commitment to staying abreast of technological advancements and exploring opportunities to enhance age assurance practices in the future. One aspect to consider is the device used to access the content. In this regard, the same levels of security and accuracy should be required, but the hardware and functionalities of devices vary. For instance, the user's mobile device offers multiple capabilities to carry out age verification through different technologies with varying degrees of precision, as it has high-quality cameras and mechanisms that can be triggered from native environments (applications) and web environments of different operating systems. This is in contrast, for example, with the hardware incorporated into a television, which typically does not have a camera. For this reason, it is proposed that any electronic device from which the user attempts to log in should allow age verification to be redirected to the mobile device. In summary, we fully support the proposed guidance's emphasis on incorporating accessibility and interoperability considerations in age assurance implementation. These principles are not only integral to fostering inclusivity and fairness but also to ensuring that age verification processes remain robust and effective in an ever-evolving digital landscape. As technology providers, we are committed to collaborating with stakeholders to further refine and enhance age assurance practices for the benefit of all users.

Question	Your response
Question 7: Do you have comments on the illustrative case study we have set out in the guidance? Do you have any supporting information or evidence relating to additional examples of how the criteria and principles might apply to different age assurance processes?	Confidential? – Y / N We find the case study to be clear and coherent with our proposal. Furthermore, our solution aligns closely with the scenario outlined in the case study and has the capability to fully address the use case. We would be pleased to share our datasheet to bolster our response and provide additional details on our solution's capabilities: https://veridas.com/docs/Datasheet-Age-Verification.pdf It's worth noting that the case study does not specify that the provider must be accredited in the United Kingdom. However, it may be beneficial to add that the vendor should be within the trusted framework/registry of DVS. This ensures adherence to established standards and regulations, enhancing trust and reliability in the solution.
Question 8: Do you agree with our proposed guidance on the record-keeping duties? Please provide any information or evidence in support of your views.	Confidential? – Y / N Veridas agrees with the proposed guidance on the record-keeping duties outlined in the document. It's crucial for service providers to maintain detailed records of their age assurance processes to ensure compliance with regulatory obligations and to demonstrate accountability in their operations. The requirement to include specific information about the age assurance process, such as details of external providers and the type of methods used, is essential for transparency and clarity. This transparency not only helps regulators and stakeholders understand the mechanisms in place but also fosters trust in the service provider's commitment to safeguarding users, especially children, from potentially harmful content. Moreover, the proposal to document how each criterion and principle outlined in the guidance has been considered and addressed is commendable. This not only provides a structured framework for evaluating the effectiveness of age assurance processes but also encourages service providers to critically assess their approaches and make necessary adjustments to ensure they are robust and fit for purpose. The suggestion to summarise the written records in a public statement adds another layer of accountability and transparency. By publicly disclosing their compliance efforts, service providers

Question	Your response
	can enhance trust among users and stakeholders and demonstrate their commitment to responsible content delivery. Overall, the proposed guidance on record-keeping duties aligns with best practices in regulatory compliance and accountability. It provides a clear framework for service providers to document and evaluate their age assurance processes, ultimately contributing to a safer online environment for all users, particularly children.
Question 9: Do you have any comments on our proposed approach to assessing compliance with the duties on service providers who publish or display pornographic content, including on the proposed examples of non-compliance? Please provide any information or evidence in support of your views.	Confidential? – Y / N We consider that the proposal put forward for assessing the compliance obligations of service providers who publish or display pornographic content, together with the suggested examples of non-compliance, is very sound. It is essential to take into account the harm or risk of harm to children when prioritising our actions in this area. The inclusion of criteria such as risk of harm or seriousness of the conduct, as well as the strategic importance of addressing the alleged offence, in the prioritisation framework is a step in the right direction. We consider that any enforcement decision should be based on the specific facts and evidence in each case. The proposal to include examples of non-compliance for each obligation in the draft guidance annexed to the guide is particularly useful, as it provides clarity and guidance to service providers on how to comply with their obligations effectively. In summary, we fully support the proposal put forward and believe that it will make a significant contribution to more effectively addressing the protection of children online. In this regard, we recognise that, as technology providers, our expertise may not be specifically tailored to address this nuanced issue and we may not be best qualified to answer this question comprehensively. However, we are open to further discussion on this issue. We would be happy to organise a meeting to discuss this and any other issues further.
Question 10: Do you have any comments on the impact assessment set out in Annex 1? Please provide any information or evidence in support of your views	Confidential? – Y / N We consider that the impact assessment contained in Annex 1 mainly affects content service providers more directly and perhaps they can provide a much more appropriate and not so generic opinion, but we would like to add that we at Veridas, as technology providers, understand that as long as the requirements for technical solutions are clear and even more so if they are subject to

Question	Your response
	assessment and certification, it will facilitate the ability of service providers to demonstrate compliance.
Question 11: Do you agree that our proposed guidance is likely to have positive effects on opportunities to use Welsh and treating Welsh no less favourably than English? If you disagree, please explain why, including how you consider the proposed guidance could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.	Confidential? – Y / N Yes, Veridas agrees. As Welsh can be used as well as English in the written records to be inspected by Ofcom, Welsh companies will have the same opportunities and will not require extra work to provide the written comments in English

Please complete this form in full and return to Part5Guidance@ofcom.org.uk.

ANNEX I

Below is a comparison of the strengths and weaknesses of various age verification mechanisms, including both the one proposed by Ofcom and those suggested in question 3, as well as others being considered in other countries.

Mechanism	Strengths	Weaknesses
Age estimation using a selfie photo	• Does not require sharing personal ID document data with the service. • No need for credential storage. Useful for services that may not require registration (e.g., adult websites). • Good user experience. • Speed in the age verification process. • Accuracy exceeding 99.9% for individuals over 25 years old.	• May be susceptible to identity theft attempts. • Cannot be carried out from all devices (for example, not feasible on a television). • Based on technologies with false positive and false negative rates. • Requires additional evidence for individuals under 25 years old to avoid errors.
Comparison with ID document	• Unambiguous age verification based on the reading of the date of birth. • Allows for complete identity verification. • Can be part of the Know Your Customer (KYC) process for service enrollment. • Requires a selfie photograph to ensure that the ID document belongs to the user undergoing the process.	• Requires access to more personal data than necessary for age verification. • May be susceptible to identity theft attempts. • Cannot be carried out from all devices (for example, not feasible on a television). • Requires support for identification documents from around the world to avoid discrimination. • The verification process may take up to 1 minute to complete.
Biometric authentication *(something you are)*	• Certainty that the person accessing the service is the one registered. • Ability to verify age each time the user accesses the service, through biometric comparison with the registered photo. • Accuracy exceeding 99.9999%. According to the NIST FRTE 1:1 report dated November 21, 2023, 150 biometric systems have a false positive rate of 0.000001 and a false negative rate below 0.005, measured in the VISA category (see report). This means the accuracy reaches 99.9999% when comparing faces of different people, while only rejecting 0.5% of cases where faces of the same person are compared and obviously attempting recognition by the system. • Biometric factors cannot be transferred or stolen. Inability to use biometric factors in other services. Privacy features by design and by default in AI-based biometric engines. • Good user experience. • Speed in the authentication process.	• Cannot be carried out from all devices (for example, not feasible on a television). • May be susceptible to identity theft attempts. • Based on technologies with false positive and false negative rates. • Requires registration in services that may not necessarily require user registration (e.g., adult pages).

Credential-based authentication *(something you know)*	• Usable from any device. • Deterministic solution.	• Not possible to ensure that the person accessing the service is the one who previously verified their age. • Possibility of password sharing or theft and use in other services. • Password forgetfulness. • Inadequate user experience. Slow process. • Requires registration in services that may not necessarily require user registration (e.g., adult websites).
Credit card *(something you have)*	• Usable from any device. • Deterministic solution.	• Possibility of a minor having access to a card. • Not possible to ensure that the person accessing the service is the one who actually obtained the card. • Possibility of theft. • Inadequate user experience. Slow process. • Sometimes, having a card is associated with having a certain income. • Requires registration of banking information in services that may not necessarily require user registration (e.g., adult websites). • May stigmatise the user of such solutions depending on the information shared with the issuing banking entities of the cards.
Age attribute credential (identity wallet)	• Based on international standards. • Privacy. Access only to the age attribute. • Good user experience. • Requires biometric authentication to ensure that the person sharing the attribute is the actual owner.	• Immature regulation and standards. • Lack of technological solutions in the market. It is a novel solution with a complex architecture that requires testing and user adoption. • Cannot be carried out from all devices (for example, not feasible on a television). • Authentication may be based on the biometric factor registered on the device (for example, FaceID, TouchID, etc.), which allows for multiple different registrations. In other words, there may be technically 'authorised' individuals to use the mobile device or application as 'age accreditation', without guaranteeing that the person using it truly has that age. In this regard, the European Banking Authority (EBA) ruled in 2023 that device biometrics should not be considered a valid element of reinforced authentication.