TECHNICAL NOTE

A SAFE INTERNET BY DEFAULT FOR CHILDREN AND THE ROLE OF AGE VERIFICATION

October 2024

CONTENTS

I. EXECUTIVE SUMMARY

This technical note from the AEPD demonstrates that **it is possible to effectively protect minors on the Internet without entailing systematic surveillance** or invasion of the privacy of all users and without exposing minors to being located and exposed to new risks. To this end, it is necessary to **change the paradigm** used until now to protect children: instead of using the current reactive strategies, it is proposed to achieve real and effective protection by applying the principle of **data protection by default**. This change in approach when designing the processing of personal data carried out on the Internet makes it possible to set up **a safe space by default for children that guarantees that they can enjoy their rights and freedoms in the digital environment**.

This note **analyses four different use cases and recommends good practices** to protect minors, and by extension all vulnerable groups, in their access to the Internet against risks related to access to content, contact with people who may put them in danger, contracting products and services, the monetization of their personal data, the induction of addictive behaviours that affect their physical or mental integrity and with other cross-cutting aspects. **All these risks have as their cause or effect the processing of minors' personal data**.

The **reactive strategies** used so far are **based on exposing children** to these risks and, in the best of cases, **reacting when it is detected that harm or impact is already occurring**. Sometimes, **protection based on Internet service providers knowing which user is a child has also been proposed**, for example, to enable the creation of specific spaces or accounts for minors. These strategies require **intrusive intervention in the form of surveillance or profiling** that systematically violates the privacy of all users: they allow the minor to be located and easily accessible to any malicious actor, they can seek to legitimize new processing of children's personal data, they adapt the messages so that they make decisions that, in many cases, do not correspond to them or may hide profiling purposes concerning deceptive or addictive patterns, engagement, contracting, consumption or monetization of personal data.

All these risks can be avoided by effectively implementing the right of minors and other vulnerable groups to **a safe Internet by default**. **Safety beyond cybersecurity** means preventing any damage to the best interests of the child and their fundamental rights due to processing their personal data so that minors, families, and other users **have control of their own data**.

Age verification is one of the tools that allow the design of this safe Internet by default, and the AEPD proposes that this age verification is **an enabler to access any element that involves risk**, acceptable to people with maturity and sufficient information, or to make decisions when they assume parental authority or guardianship of a minor. In addition, **keeping the burden of proof on the user at the appropriate age and never on the child**, avoiding the creation of identity schemes for minors controlled by different service providers.

Age verification, per se, is not enough to guarantee a safe Internet by default. It needs to be **designed and implemented in a way that meets all the principles and requirements set out in the GDPR**. In addition, **Internet services and apps should be adapted** to perform age checks and to integrate other solutions to make minors' protection effective while avoiding generating new risks, such as allowing minors to be located or its use entailing any loss of rights or freedoms.

II. INTRODUCTION

The Internet offers educational, social or creative opportunities for minors. However, within the framework of the processing of their personal data, **new risks associated** with inappropriate content, cyberbullying, exploitation, addictions, or consent to specific activities or operations can be materialized against them. Other risks that affect children involve considering them as passive subjects, which can be **directed, manipulated or converted into captive customers** in the long term or treated as **monetizable products through** their **"datafication"**. The protection of the **best interests of the child** must be **a priority in the digital environment** as it is in the physical world.

Data protection regulations establish principles, rights, and obligations concerning the processing of personal data in general and **with greater guarantees regarding the personal data of minors**. These imply specific compliance obligations that legitimize processing and manage risks to the rights and freedoms of minors and all Internet users.

The **strategy followed so far to protect children** on the Internet by most providers of digital products has been **reactive**: allowing children to be exposed to these risks through the processing of their personal data and, in the best of cases, reacting when it is detected that damage or impact is already occurring. This involves **exposing the minor** to, for example, any user being able to contact them, subjecting all users to monitoring and profiling techniques, accumulating evidence of harassment, grooming, paedophilia or others, applying criteria established by the provider and finally acting. This strategy requires proof of harm to the child for protection measures to be activated. In addition, for it to work, **intrusive intervention in the form of surveillance or profiling** is often necessary, something that systematically violates the privacy of all users. Other strategies are based on **enabling Internet service providers to know who a minor** is or their specific age. For example, when particular spaces or accounts are offered for minors. In this way, the provider intends to configure and monitor the minors' activity while using its service or adapt the messages so that they can make decisions (which, in many cases, do not correspond to them).

Implementing these strategies requires **the intrusive intervention of Internet service providers in the form of surveillance or profiling** that systematically violates the privacy of all users. In addition, they involve **having the minor located and easily accessible** to third-party services or, directly, malicious actors. This strategy **may seek to legitimize a massive processing of children's personal data and all users.** In addition, they may **conceal profiling purposes** concerning deceptive or addictive patterns, engagement, consumption, or monetization of personal data. In many cases, they also intend to create **new digital identity schemes**, considering identity as a service rather than a right. These schemes initially applied to children, would be the ones that would be extended in the future, given that users who are now minors will become adult users later.

These risks can be avoided by making effective the right of minors and other vulnerable groups to a **safe Internet by default**. Safety means **more than security**; safety means preventing harm to the best interests of the child and their fundamental rights due to the processing of their personal data when it is not necessary, that is, not only to protect their personal data from unauthorised processing, loss, destruction or damage. **Minors must also be protected from the risks produced by the "authorised" processing of personal data, which** are the cause or effect of risks to their physical and mental integrity. It also means giving back to the minor and to those who hold parental authority or guardianship the power to make decisions about their own data, which implies being able to decide to what extent the minor is exposed to potentially harmful contacts, contracts, behaviours and content.

A safe Internet by default must be built **from the design** and following the principle of data minimisation since the processing of children's personal data, location, and accessibility are some of the leading causes of risk. It is not enough to include an additional layer of security

on Internet services as they are currently implemented, but **Internet service providers must** evolve to **implement data protection principles by design and by default**.

Age verification is one of the tools that allows the design of a safe Internet by default, although it is not the only one, nor can it provide a solution to all the challenges that this design implies on its own. Age verification should be understood as an **enabler to access any element that involves a risk** acceptable to people with maturity and sufficient information or to make decisions when they assume parental authority or guardianship of a minor. In this way, **the child must not prove that they are a child**, nor expose their nature so that content, contacts, contracts or functionalities are blocked, nor receive information to be able to make decisions that do not correspond to them. On the contrary, this **proactive approach** gives back to family members and guardians the ability to exercise their responsibilities concerning duty of care and shifts **"the burden of proof"** of exceeding an age threshold to expose oneself to risks and of the willingness to do so to the adult, as established in Article 8 of the GDPR and Article 7 of the LOPDGDD. It must also be done **by default** to be effective.

With a safe Internet by default, a minor's status or age is not exposed or addressed. The processing of children's personal data, including their status as minors, is not necessary, proportional and, in many cases, is not fair. **The burden of proof of being able to perform a particular activity on the Internet rests with the user of the appropriate age for it. It will be an adult user who selects those elements (with the associated risks) appropriate to the child's maturity level under their guardianship**. The type of content that a minor can access, their contacts, the contracts they can enter into or the functionalities of the services they can access are decisions that the regulations assign to those who hold parental authority or guardianship, who are the ones who must prove their capacity to act and to whom the information that allows them to make an informed choice must be addressed, not to the child.

Technology must be designed and implemented to provide solutions without creating new threats or violating the rights and freedoms of all users. In particular, age verification **must not create new risks, either for individual subjects or in the form of systemic risks** for society as a whole.

The Internet ecosystem **cannot be treated as a set of independent silos**. Suppose the goal is to implement **a paradigm shift in** the protection of children. In that case, it is necessary to establish **cooperation between all the parties involved** (suppliers, manufacturers, intermediaries, etc.) when designing their solutions, but also to **effectively communicate** with each other and with the rest of society in the face of the identification of new threats through a **governance framework.**

For this reason, this note is aimed at **providers, manufacturers, intermediaries and other Internet operators**, as well as **data protection and consumer authorities and those competent in the regulation of the market**, especially for products and services offered on the Internet and to **governmental and non-governmental** organizations whose purpose is the education and protection of minors, both Spanish and European. Of course, it is also aimed at those **responsible for personal data processing** who consume or use these products and services offered on the Internet and those **with parental authority or guardianship** of children.

III. BACKGROUND AND CONTEXT

A. OBLIGATIONS WITHIN THE INTERNET ECOSYSTEM

Different actors such as parents, educators, governments, regulators and judicial or supervisory authorities **must assume their corresponding obligations** to ensure that minors can take advantage of the opportunities offered by the digital space while being **adequately protected from the risks** it implies. In particular, members of the technology industry must assume their obligations in the protection of children in a way that complies with current regulations, in particular **compliance with data protection regulations**, either as controllers or processors and be more ambitious by incorporating proactive tools and adapting processes that allow the aforementioned actors to exercise their different responsibilities. In addition, it should be noted that **Article 28 of the Digital Services Regulation** states that online platforms that minors may use must ensure that their services offer a high level of privacy, security and protection to younger users.

Internet service providers, and to the extent that they are responsible, the rest of the actors in the Internet ecosystem (manufacturers, other providers, intermediaries, etc.) must provide **an environment that is safe by default for children** without arrogating to themselves functions that correspond to parents, educators, governments, regulators and judicial or supervisory authorities. Minors' protection will be at risk if it is intended to prevent them from exercising their obligations to monitor, care for, and educate children. **Their different responsibilities cannot be delegated**, nor should they be based on "leaps of faith", especially on Internet actors whose interests, given their current business model, may collide directly with the **protection of the fundamental rights of all users**.

When this happens, **hyper-surveillance** is usually deployed, involving the massive processing of all citizens' personal data, profiling, detection of minors in, by, and through digital services, loss of control of personal data (recital 7 of the GDPR), and, in the worst case, manipulation (through deceptive and addictive patterns) for monetization purposes.

B. SAFETY BY DEFAULT AND BY DESIGN

Until now, the responsibility for preventing risks to minors on the Internet has rested mainly with **the children themselves, as well as their parents and educators**. Providers and other participants in the digital ecosystem have primarily focused on developing **reactive strategies**. These strategies involve **taking action after minors have been exposed to risks** or once damage or impacts have occurred. An example is the potential (and even the encouragement) for anyone to initiate contact with a child through a service or platform without the default control over who can make this contact being in the hands of those with parental authority or guardianship. Alert mechanisms are only activated, following the service provider's criteria, in the event of evidence of some form of harassment.

This approach risks the child's best interests and fundamental rights. It also threatens the fundamental rights of other Internet users, as it relies on surveillance and profiling conducted by service providers to identify risk situations using criteria they have established. It involves unnecessary personal data processing that infringes **the minimisation principle**. This approach means that the reaction, if it occurs at all, happens once damage that may be irreversible is done, so a necessity test is not passed. The data processing is ineffective as it does not meet its purpose adequately.

Reactive measures have been justified in the past because digital products have been designed to make it difficult, or directly impossible, for parents, educators, governments, regulators, judicial authorities or supervisory authorities to exercise their share of responsibility. All these digital products **facilitate from the design, or even encourage, minors to be users**. Once they are, it is up to the providers to perform the necessary data processing to deploy this type of reactive measures. This could be **a breach of the principle of fairness**. Fairness is a general principle that requires that personal data not be processed in a manner that is unjustifiably harmful, unlawfully discriminatory, unexpected or misleading to the data subject[1].

Taking the physical world as an example, to guarantee the right of minors to move freely on the streets, they must be safe by default and always do so under adult supervision. Parents, educators, governments, regulators and other authorities must have the necessary resources to exercise their responsibility and establish, in each case, the *a priori* measures that avoid the main elements of risk.

However, a higher level of protection cannot be claimed in the digital environment than in the physical environment or with a lower level of participation or involvement of the already mentioned agents (parents, educators, governments, regulators, judicial authorities, supervisory authorities) to achieve it. This requires a **holistic vision** of the child's best interests and the protection of their fundamental rights, i.e., a safe Internet by default cannot be limited to specific aspects (access to inappropriate content, addiction, etc.), nor consider them unconnectedly. Still, **all rights must be regarded as unified without establishing a hierarchy or priority**.

It is essential to consider that keeping minors safe on the Internet is directly tied to the concept of safety. We need to ensure that, in the name of biased or misunderstood security (cybersecurity), we do not compromise the child's best interests or violate their fundamental rights. **Safety is not solely about security** or cybersecurity; it is not only about making sure that the information associated with a child's online activity is protected against accidental loss, destruction, or damage. **Although security is a crucial factor in achieving safety, you cannot equate the two**; this is a simplification that leads to mistakes, such as thinking that a single measure or strategy can solve the problem. In fact, a high degree of cybersecurity can be achieved without protecting minors, even with severe impacts on their rights and freedoms.

C. AGE VERIFICATION

While protecting children is crucial, it must always be compatible with the **rights and freedoms of all citizens**. This protection can be achieved with an **appropriate combination** of different methods, tools, and processes, among which age verification plays a crucial role **in strictly respecting all users' fundamental rights**.

Age verification solutions make it possible to **determine if a user is over the minimum age required to pass an online age gate**. For example, if a user is over 18 years old, needed to play a video game classified as violent or to configure a messaging *app* so that messages can be received from any other user without limitations. As developed in this technical note, this type of solution ensures that the user accessing age-restricted content, contacts, contracts or functionalities is of the required age to do so.

[1] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

The GDPR requires compliance with the **principle of accuracy** of data concerning the purposes for which it is processed (Article 5(1)(d)). Insofar as it can limit fundamental rights, age verification **must be accurate in terms of suitability to fulfil its purpose**: to grant access to some elements of the Internet that imply a risk for minors. This does not mean that the processing of the date of birth of Internet users by providers of digital products is always necessary. Collecting the date of birth or precise age of Internet users when not required infringes the minimisation principle. In most use cases, it will be sufficient to know if the user **exceeds an age threshold** or, in the case of using trusted third parties through tokenised architectures[2], simply **if they are able to access** the element they are requesting with a "exceeds the required age threshold", "YES", "OK", etc.

The approach to applying age verification should always be **enablement**, i.e., to demonstrate that the age threshold is exceeded and that the requested operation can be carried out. In this way, the risk to minors is limited, data minimisation is applied, and the processing is proportional by avoiding processing children's personal data, issuing specific attestations or certificates for them, installing applications on their devices, etc. Digital products must protect minors **by default and design**, preventing them from taking risks and not waiting until they are exposed to them to react and try to mitigate them. In this sense, age verification can be a very useful tool.

For this reason, this technical note explores the use of age verification solutions for child protection on the Internet, as it is one of the tools with the most potential to implement age-related protection. However, it has **significant implications for privacy and data protection**. Indeed, as it is likely that, due to its nature, scope, context or purposes, age verification entails a **high risk to the rights and freedoms of individuals**, the controller of personal data associated with this verification must carry out before processing, **an assessment of the impact that such processing has on the protection of personal data**.

D. SYSTEMIC RISKS

Regarding these implications for rights and freedoms and the concept of risk, it should also be avoided that age verification solutions could **significantly impact society**, the economy or security because of their broad influence or **ability to affect a large number of users**. These risks could occur if the provider of a verification solution is given the power of a monopoly or the ability to profile a significant number of Internet users or if a breach in its security could affect the sensitive data of that substantial number of users[3].

Risks to the child's best interests and the rights and freedoms of all citizens should be avoided, as well as **the systemic risks** that a given design or implementation of age verification solutions may entail, given their potential scale. A risk **is systemic when it can cause damage to people on a large scale or systems essential for the governance and proper functioning of society**.

According to the Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) there are four **categories of systemic risks** (recital 80). Two of them are very closely related to the processing of personal data that is carried out in age verification solutions.

---

[2] In this type of technological architecture, a trusted third-party provider specialised in carrying out age verification is the one who performs the appropriate checks with the user, so that the provider of the application or service only receives a token or credential that proves that the user exceeds the required age threshold, no other data.

[3] Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

The second category identified in the Regulation (recital 81) concerns **the actual or foreseeable impact of the service on the exercise of fundamental rights**, as protected by the Charter. If age verification solutions are not adequately designed and implemented, many of these rights can be violated, including freedom of expression and information, respect for private and family life, the right to data protection, and the right to non-discrimination.

Specifically, and concerning the right to data protection, the protection of minors is sometimes used as a **justification for the mass collection** of data from children and other users on the Internet: mass profiling, categorisation of content and users, evaluations or automated decisions, etc. In some cases, age verification solutions are proposed as solutions for **digital identity management** for Internet users. Such an identity, provided and managed **as a service rather than a right**, is not under the control of the users themselves but depends on the criteria and interests of a provider who may, at its discretion, eliminate that identity or limit the ability of individuals to act.

Creating a safe Internet by default for minors cannot, in any case, be the alibi for this massive processing of personal data that does not comply with the principles of fairness, transparency, or data minimisation and would infringe on different rights and freedoms. **Given** its potential scale and scope, this risk would be systemic.

In addition, it should be taken into account that an age verification solution that monopolises a large part of the market could lead to **a lack of timely availability of access to content, services, contracts**, etc., affecting not only different rights and freedoms but also the **resilience of the digital infrastructure and the economy**.

The third category of systemic risks (recital 82) refers to **actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, as well as public security**. It should be considered that, due to their scale and level of intermediation in information flows, certain services and applications have become public spaces with a central role that facilitates public debate, access to information or economic transactions, to mention a few examples. The potential harm to individual users, but also society, of poorly designed and implemented age verification solutions from the point of view of their suitability is enormous (errors, biases, exclusion, etc.). Again, **creating a safe Internet by default for children cannot, in any case, be the alibi for limiting access** to these services and applications in breach of the principles of lawfulness, fairness or accuracy, and that would violate different rights and freedoms. **This risk would also be systemic**, given its potential scale and scope.

While these two categories of systemic risks are what age verification solutions can cause if not properly designed or implemented, there is another angle for analysis: **not performing age verification at all or doing it in a way that is not suitable can also imply systemic risks**. The fourth category of risks identified by the DSA derives from the **design, functioning or use, including through manipulation, of very large online platforms and of very large online search engines with an actual or foreseeable negative effect on the protection of public health, minors and serious negative consequences to a person's physical and mental well-being, or on gender-based violence**. As established in this technical note, age verification does not entirely prevent these risks to minors' physical and psychological well-being, but it is a fundamental tool for their protection. Therefore, in some instances, not carrying out age verification at all or carrying it out in a way that does not fulfil its function can also pose a systemic risk, mainly when such a system allows children and adolescents to be identified and detected on the Internet.

E. CATEGORIZATION OF RISKS TO CHILDREN ON THE INTERNET

To understand how age verification can help protect minors online, it is first necessary to understand what exactly they need to be protected from. This note uses the OECD classification[4], so that five categories of risks (the five Cs) are considered:

1. Content: Hate content (based on race, gender, religion, sexual orientation, etc.), harmful content (pornography, extreme violence, substance use, extremism, eating disorders, etc.), illegal content (sexual abuse, terrorism, etc.) and misinformation can have an impact on the mental health and emotional development of minors.

2. Conduct: Again, the four types of risks already mentioned are observed, but in this case, they refer to the behaviour of the minor themself when using the Internet, which can place them in a vulnerable position for participating in hateful (cyberbullying, etc.), harmful (sexting, etc.), illegal behaviours or participating in the distribution of misinformation.

3. Contact: There are risks in similar categories, but in this case, minors are contacted by someone who interacts with them through the Internet and makes them the target of hateful, harmful, illegal or problematic messages for other reasons. Some clear examples are sextortion, grooming or situations in which minors provide enough data to move from contact in the virtual world to contact in the physical world, with a risk to their right to integrity. The difference with Conduct risks is that, in this case, the minor is a direct object or victim rather than an actor or active party.

4. Consumer (contract or consent): These occur when the minor is a customer or consumer, mainly because they receive advertising for products that are not suitable (such as tobacco, alcohol or dating services); because they receive advertising that they cannot identify as such (for example, by product placement or through an influencer); because their credulity, inexperience, or lack of maturity is exploited to make them consent to agreements or contracts that are not beneficial to them (e.g., by employing deceptive patterns) or because, directly, it is not up to the minor to make decisions about consumption, contract or consent[5].

5. Cross-cutting: This category includes traversal and heterogeneous risks that cannot be classified into the previous categories, mainly:

a. **Privacy risks:** Such as over-exposure caused by themselves, sharenting, processing associated with educational technologies and platforms, etc.

b. **Advanced technology risks:** Such as those associated with the use of artificial intelligence (for example, tools that produce fake nude photos offered in video game chats), the Internet of Things (for example, children's smart watches that allow geolocation), the processing of neurodata (for example, to play video games or monitor attention in class) or biometric authentication (for example, to pay in school canteens or to access a sport event).

c. **Risks on health and wellbeing:** Such as those associated with addictive patterns used by some services and applications or excessive screen time.

Once the main risks faced by minors on the Internet are understood, the following statements can be made, which will be supported throughout this document:

[4] "CHILDREN IN THE DIGITAL ENVIRONMENT: REVISED TYPOLOGY OF RISKS", OECD Digital Economy Papers, January 2021 No. 302. https://www.oecd-ilibrary.org/science-and-technology/children-in-the-digital-environment_9b8f222e-en

[5] Article 7 GDPR and Spanish LOPDGDD.

- Age verification solutions, with the right **model**, can greatly help avoid or mitigate many of these risks **by design and by default**.
- The selection of the suitable model for age verification and its design and implementation must be based on a **Child Rights Impact Assessment (CRIA[6])**. Managing risks for children on the Internet should not be done mindlessly or in a rigid or standard way but rather after a **systematic and specific assessment** of the five categories of risks already mentioned in the case of a particular application or service, both for its functionality and for its target audience, context of use, etc.
- Age verification can use to manage all these risks, the **enabling approach** that checks that the user exceeds the age threshold required to make changes to the configuration, allow access to communication with third parties, install applications for adults, etc.
- This allows **risks to be managed proactively** and allows parents and guardians to exercise their responsibilities.
- Age verification **does not need to verify a specific age or date of birth**, only that the threshold has been exceeded. This threshold may differ depending on the type of activity or element to be accessed on the Internet.
- Age verification **is useless if the entire ecosystem (applications, tools, interfaces, etc.) is not adapted to** protect minors by default and to verify that users who make specific requests are of the required age to do so in such a way that anonymity, non-traceability and the detection of minors are guaranteed.

The rest of this technical note analyses **the four most widespread use cases today**, as described in Table 1, to conclude with a discussion on the principles that must be applied in relation to privacy and data protection so that they guarantee not only the protection of the minor's best interests, but also the rights and freedoms of all citizens and that no new systemic risks are generated.

Use case	Risks that can be avoided or mitigated by age verification
1.Protection from inappropriate content	Content
2.Safe environments for childhood	Content+Conduct+Contac+Cross-cutting
3.Online consent for personal data processing	Consumer (contract or consent)
4. Age-appropriate design	Conduct+Consumer (contract or consent) + Cross-cutting

Table 1. Use cases analysed in this note

The following sections of this note will discuss how age verification is an essential tool to avoid or mitigate many of these risks, but it is not the only one in any case; it must be integrated and complemented with other types of tools, solutions and processes (figure 1) in a child protection system.

[6] "CHILD RIGHTS IMPACT ASSESSMENTS IN RELATION TO THE DIGITAL ENVIRONMENT: DEVELOPING GLOBAL GUIDANCE", UNESCO, April 2024. https://www.unicef.org/reports/CRIA-responsibletech

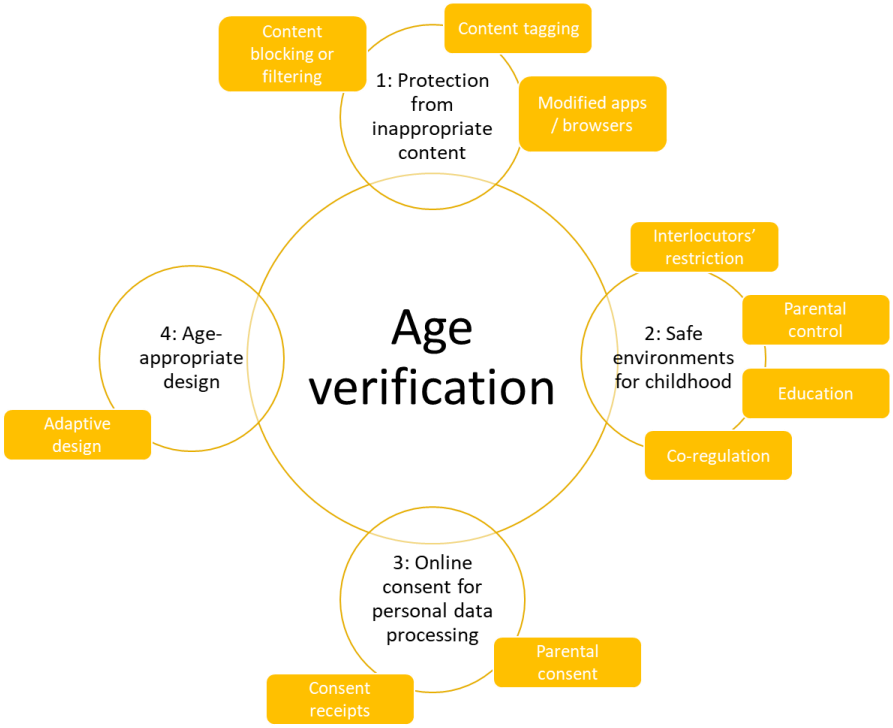

Figure 1. Age verification and other solutions across use cases

IV. AGE VERIFICATION MODELS

One of the fundamental decisions that must be made to perform age verification correctly is that of its **timing**. Age verification can be carried out **at different times** during a user's interaction with services and applications, so the responsibility for carrying it out falls on other actors. Those performing age verification can do so with their own solutions or by relying on solutions offered by trusted third parties. However, this document does not discuss the different architectures or possible methods to do so.

In any case, a design principle must be complied with: age verification must be carried out in the context of access to the service or application **before any other processing of personal data is carried out**. In other words, users' personal data should not be collected and access denied because they do not meet the age requirements.

Otherwise, two different models can be distinguished.

A. ADULT SERVICES AND APPLICATIONS

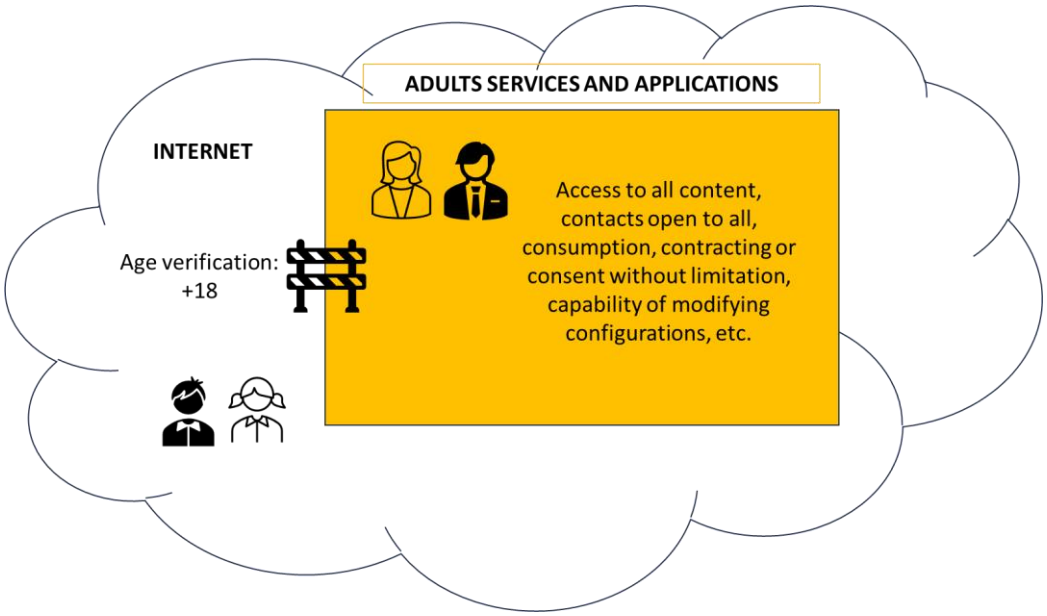

Figure 2. Age verification within adult services and apps

All users are adults, in no case children, who should not be able to access the service or application given their nature and the risks it implies.

Who should implement age verification? If it is an app, the corresponding store should verify that the user who wants to download and install the app exceeds the required age threshold (usually +18). Since there are other means of downloading and installing applications, it could also be the provider of the service accessed through the app that performs the appropriate checks, for example, the first time an access is made. If it is a service that can be accessed through a web browser, the service provider should check whether the user exceeds the required age threshold before creating an account or performing an isolated access. The browser should provide all the necessary support to perform this check properly.

When is the age verified? In this model, age verification is the entry enabler for using the service or application: to start using it, one must demonstrate that the required age is exceeded. This process should be done at least once, in the store or with the provider, to download the app or create an account.

Is refreshment required? The answer to this question depends on the right balance between different factors: the risk of inferring the users' status as minors, the risk that access to inappropriate content poses to children, and the risk of manipulating age verification procedures or usability.

As mentioned above, age verification should always be done at least once to download the app or create an account. It may then be repeated when certain events occur, e.g. device events such as SIM reboots or changes, changes to functionalities or terms of service that may affect age requirements, modifications to user account information such as email, for example (to prevent the transfer of accounts between users), etc. If the service allows guest access (without creating an account), age verification should be carried out during each session.

Example of good practice 1

A dating mobile app is suitable for adults only; you must be 18 or older to install it.

The official app stores verify users' age before allowing them to download and install this app.

They perform the verification again on each update of the app.

Example of good practice 2

A porn website is only for adults; you must be 18 years old or older to be able to create an account and be able to access the content it offers.

The page provider verifies age before allowing the user to create an account.

Age is verified again with each update of the information associated with this user account, such as username or email address.

Example of bad practice 1

A gambling website is for adults only. You must be 18 years or older to place bets. No other content or services are offered on the website.

The website provider allows all users to create an account and, therefore, processes the personal data associated with this account creation for all of them without verifying their age. The provider does not verify age until the user tries to place a first bet.

The personal data processing of users under 18 is completely unnecessary at the time of account creation, as they are not allowed to access the service for which the account was

created. The mistake is in the poor design decision as to when the age verification should be performed.

Example of bad practice 2

A generalist content website is for all audiences. It does not offer any other type of content or service that can be classified as "for adults", and no consent is requested to process personal data.

However, the provider decides to carry out age verification on all its users to collect new data (at least, age) and to be able to personalize content, advertising, etc., depending on the age range to which they belong. Again, this personal data processing is neither necessary nor proportional. The mistake is in the poor design decision regarding the realization of age verification in a site for all audiences that does not imply significant specific risks for minors.

B. MIXED SERVICES AND APPLICATIONS (FOR ALL AUDIENCES)

In this case, users can be both children and adults. Some content, functionalities or configurations are considered suitable for all users while others are considered inappropriate for children due to the risks they may pose and must be protected by age checks.

In this case there are two design alternatives.

1. The provider offers two versions of the service or application (age separation)

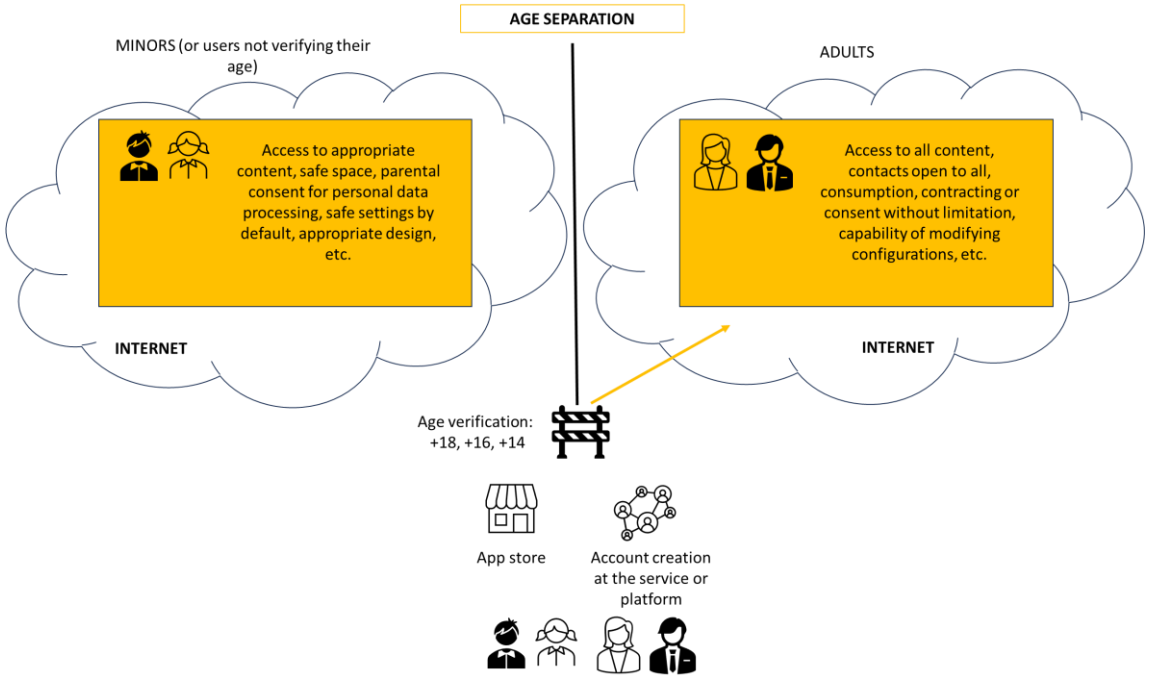

Figure 3. Age verification within mixed services and apps based on age separation

The provider offers two different experiences in its service or application. One version implies protection by default for all users so that it only allows access to content, functionalities, configurations, and safe elements for all audiences without age restrictions. The other does not imply this type of protection by default, and the user uses it despite the risks it may imply. To do this, you must exceed an age threshold and prove it.

Who should implement age verification? If it is an app, the relevant store should verify that the user who wants to download and install the not-safe-by-default version of the app exceeds the required age threshold (usually +18). If the store is not ready to perform this type of age verification, the app provider might offer a single version for all users to download, which provides protection by default. Once downloaded, it incorporates a configuration option for which it is necessary to verify age with the app provider, which disables all protections globally. This makes the app the version that does not offer protection by default after a single age verification process.

If it is a service that can be accessed through a web browser, the service provider should check that the user exceeds the required age threshold with the support provided by the browser before creating an account without default protection.

In any case, if the user cannot prove that they are over the required age, either with the store or the provider, they will be able to access the app or the account, but always with protection by default.

When is the age verified? As in model 1, age verification is the entry enabler to access the service or application, in this case, in its version without protection by default. This process is usually carried out at least once in the store or with the provider.

Is refreshment required? Same as in Model 1.

Example of good practice 3

A social network decides to offer two different versions of its application. The first implies protection by default for all users, so minors can use it without posing a risk to them: it does not allow access to content with age requirements, it limits the options for contact with other users (for example, through allow-lists), it does not process personal data, it has all the safe options configured by default, etc. The other version of the application does not include these protections by default, so it implies a risk that adults can only assume.

All users can install the version with default protection without age verification. However, the official app stores require age verification before allowing users to download and install the version that does not perform protection by default.

They perform the verification again on each application update to a new version.

Example of good practice 4

A live video streaming service offers safe-by-default and adult accounts. Safe-by-default accounts do not allow access to transmissions from other users with age restrictions, limit the options for contacting other users (for example, through allow-lists of contacts or interlocutors), do not process personal data, do not allow the monetization of shared

content, have all safe options configured by default, etc. All these protections are not offered by default on adult accounts.

Age verification is not required to create safe-by-default accounts. However, the service provider performs age verification before allowing the user to create an adult account.

They recheck age once a month, regularly.

Example of bad practice 3

A social network decides to offer children's accounts and adult accounts. Children's accounts involve private profiles by default, do not allow access to content inappropriate for children, limit the options for contact with other users (for example, through allow-lists of contacts or interlocutors), do not process personal data, do not allow the monetization of shared content, have all safe options configured by default, etc. All these protections are not offered by default on adult accounts.

Creating adult accounts does not need age verification, but creating child accounts does. The social network provider verifies age before allowing the user to create a new child account.

This implies a risk of detection and location of minors (by a malicious provider, dishonest employees, third parties who access the data in an unauthorized manner after a data breach, etc.) and makes the processing not proportional. The mistake is in forcing minors to verify their age; the default account must always be the one that is safe by default for all users. Age verification must be aimed at verifying that the user willing to take a particular risk is of the required age to do so; it is an enabling process for this.

2. The provider offers a single service or application with protection by default for all users

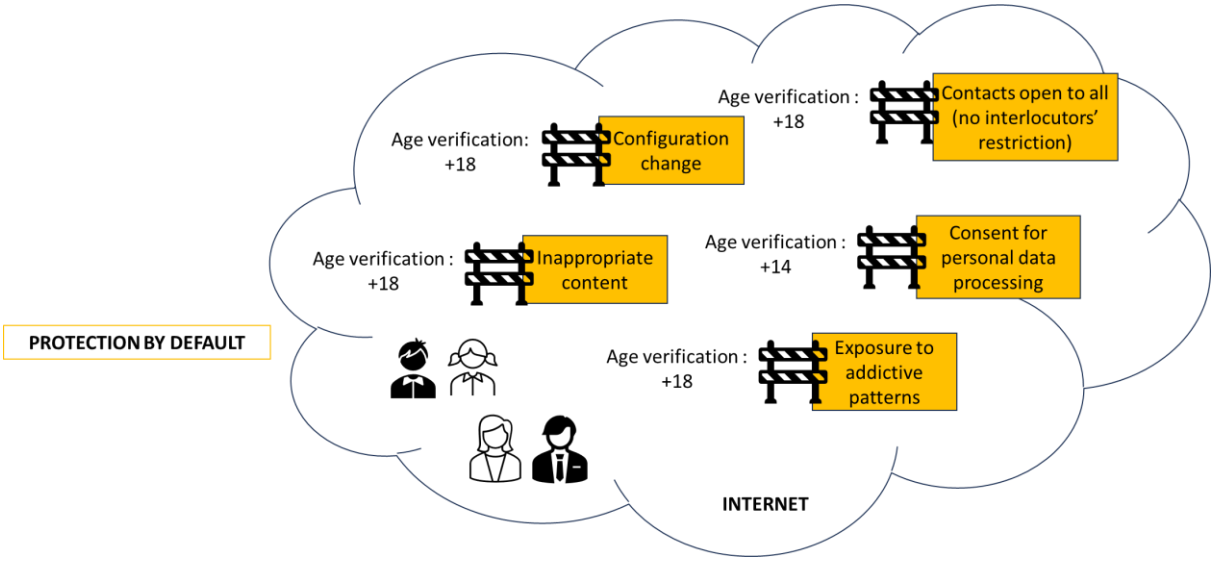

Figure 4. Age verification within mixed services and apps based on protection by default

Sometimes, the user's interaction with the service is punctual, anonymous, does not involve any type of download or creation of an account, etc. In this case, model 1 from before is not possible, and the provider cannot separate user experiences by age. Specific age checks should then be carried out during the interaction with the service or application.

Who should verify age? The only version of the service or application should guarantee protection by default for all users. When a user decides that they want to have access to age-restricted content, functionalities, or configurations, the provider, due to the risks involved, should verify specifically that the user exceeds the required age threshold for that request. It should do so with each request for content, functionality or configuration that, due to the risk it entails, requires exceeding an age threshold.

When is the age verified? In this case, age verification is likely to be performed more frequently whenever the user wishes to access adult content, functionality, or settings. The service or application provider performs this age verification since the same version of the app is always downloaded in the stores (the only one available, with default protection for everyone) regardless of the user's age.

Is refreshment required? Age verification should be carried out whenever a user requests content, functionality or configurations with age restrictions. If you want to avoid this, you could implement "reusable" verifications, somehow associating age verification to the device in the case of apps or integrating it with user session management in the case of services. This way, if the user has verified that they are over 18 to access adult content, they can avoid performing this verification again to see other adult content right after, on the same device or during the same session. However, these are particular design decisions for each provider.

Example of good practice 5

A communication and messaging provider offers all users a single version of the app in the store. All users can download and install this app without age verification.

The app incorporates safe settings by default (no user information is displayed, location is not shared, personal data is not processed, contacts are limited by the Contacts list, messages from other users that have not been previously explicitly approved are not shown, etc.). If a user wishes to modify any of these settings, they have to prove, each time, through an age verification process carried out by the app provider that they are old enough to do so. For example, they will need to do this in order to receive messages from any user or to start sharing location.

Example of good practice 6

An e-commerce platform does not, in principle, distinguish between users depending on their age. All users can browse its website and make purchases without having an account as a guest.

However, this platform provider carries out an age verification process before showing information about products unsuitable for children, such as tobacco or alcohol.

If a user proves that they are old enough to access information about these products, this information is associated with their session cookie, so there is no need to carry out an

age verification again throughout the session. Each platform could configure the duration of the sessions according to its specific needs.

Example of bad practice 4

A video game platform offers a single account version for all users without age verification.

Safe settings can be locked by default (no user information is displayed, no location sharing, no personal data is processed, contacts are limited and messages from other users that have not been explicitly previously approved are not shown, access to video games with inappropriate content is restricted, etc.) for a specific account if it is verified that it is for a child. It can be done by the children or their parents or guardians exercising their duty of care.

This implies a risk of detection and location for minors and means that the processing of personal data involved in age verification is not proportional. The mistake is in forcing children to verify their age to be protected when the safe option should always be the default option: it must always be verified that the user exceeds the age threshold required to carry out an activity that involves a risk for minors (age verification is an enabler), and not the other way around.

V. USE CASE 1: PROTECTION FROM INAPPROPRIATE CONTENT

A. PRELIMINARY FRAMEWORK

Uncontrolled access to inappropriate content by minors is one of the main concerns of parents and educators today. For this reason, different agents are working to protect minors from this content without risking their physical integrity or safety and without subjecting them to surveillance or monitoring. Nor to other Internet users, since **all content must be freely accessible to those who can demonstrate that they are over the established age threshold** while respecting their fundamental rights and freedoms.

In December 2023, the Spanish Data Protection Agency published different materials in relation to its project related to this use case. Specifically, an Infographic with the threats and risks to the rights and freedoms associated with age verification systems in this use case and a Decalogue of Principles that age verification systems must comply with when they are used to protect minors from inappropriate content. Other **European data protection authorities** (CNIL, [7]Garante per la protezioni dei dati personali[8]) as well as audiovisual market regulators (Arcom[9], Agcom[10]) have also recently published their proposals and conclusions. In addition, the **European Commission** is working on offering a **harmonized solution** in the member states with different initiatives[11].[12][13]

B. LEGAL FOUNDATIONS

The following European and national regulation includes the need to protect minors from inappropriate content, pointing out in some cases as the most harmful those that show gratuitous violence or pornography.

GDPR **recital 38**	Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child..
GDPR	The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular:

[7] https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors
[8] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9965235
[9] https://www.arcom.fr/vos-services-par-media/consultations-publiques/consultation-publique-sur-le-projet-de-referentiel-determinant-les-exigences-techniques-minimales-applicables-aux-systemes-de-verification-de-lage-mis-en-place-pour-acces-contenus-pornographiques-en-ligne
[10] https://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_FnOw5lVOIXoE&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_count=1&_101_INSTANCE_FnOw5lVOIXoE_struts_action=%2Fasset_publisher%2Fview_content&_101_INSTANCE_FnOw5lVOIXoE_assetEntryId=33778802&_101_INSTANCE_FnOw5lVOIXoE_type=document
[11] Better Internet for Kids: https://www.betterinternetforkids.eu/
[12] Digital Services Act: Task Force on Age Verification: https://digital-strategy.ec.europa.eu/en/news/digital-services-act-task-force-age-verification-0
[13] European Board for Digital Services: https://digital-strategy.ec.europa.eu/en/policies/dsa-board

recital 75	where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.
(SPANISH) Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual **article 88**	Los prestadores del servicio de intercambio de vídeos a través de plataforma adoptarán medidas para proteger: a) A los menores de los programas, de los vídeos generados por usuarios y de las comunicaciones comerciales audiovisuales que puedan perjudicar su desarrollo físico, mental o moral.
(SPANISH) Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual **article 89**	1. Los prestadores del servicio de intercambio de vídeos a través de plataforma, para proteger a los menores y al público en general de los contenidos audiovisuales indicados en el artículo anterior, tomarán las siguientes medidas: a) Incluir y poner en práctica en las cláusulas de condiciones del servicio de las plataformas de intercambio de vídeos las obligaciones establecidas en el artículo 88 sobre determinados contenidos audiovisuales. b) Establecer y operar mecanismos transparentes y de fácil uso que permitan a los usuarios notificar o indicar al correspondiente prestador los contenidos que vulneren las obligaciones establecidas en el artículo 88. c) Establecer y operar sistemas a través de los cuales los prestadores del servicio expliquen a los usuarios el curso que se ha dado a las notificaciones o indicaciones a que se refiere la letra anterior. d) Establecer y aplicar sistemas de fácil uso que permitan a los usuarios del servicio calificar los contenidos que puedan vulnerar las obligaciones establecidas en el artículo 88. e) Establecer y operar sistemas de verificación de edad para los usuarios con respecto a los contenidos que puedan perjudicar el desarrollo físico, mental o moral de los menores que, en todo caso, impidan el acceso de

	estos a los contenidos audiovisuales más nocivos, como la violencia gratuita o la pornografía. f) Facilitar sistemas de control parental controlados por el usuario final con respecto a los contenidos que puedan perjudicar el desarrollo físico, mental o moral de los menores. g) Establecer y aplicar procedimientos transparentes, eficaces y de fácil uso para el tratamiento y la resolución de las reclamaciones de los usuarios a los prestadores del servicio, en relación con la aplicación de las medidas a que se refieren las letras anteriores. h) Facilitar medidas y herramientas eficaces de alfabetización mediática y poner en conocimiento de los usuarios la existencia de esas medidas y herramientas. i) Facilitar que los usuarios, ante una reclamación presentada por ellos y no resuelta satisfactoriamente, puedan someter el conflicto a un procedimiento de resolución alternativa de litigios de consumo, de acuerdo con lo previsto en la Ley 7/2017, de 2 de noviembre, por la que se incorpora al ordenamiento jurídico español la Directiva 2013/11/UE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo. Todo ello sin perjuicio de que los usuarios puedan acudir a la vía judicial que corresponda.

C. A FIRST APPROACH

The best way to address this use case is to **ensure that anyone accessing age-restricted content is of the required age**. This approach prioritizes the child's best interests and the rights and freedoms of all users. Where a user cannot prove that they are over the required age, the content must be filtered or access to it blocked using the chosen method, outside the scope of this technical note.

In the case of **adult services or applications** that require verification that the user is over 18 years of age, it is already known that said user is of the right age to access any content that may be offered. In other words, it is model A of section IV of this document.

Two scenarios are possible for services or applications for all audiences that offer hybrid or mixed content (some with age restrictions, others not). These are explained in models B.1 and B.2 of section IV.

It is worth remembering that **age verification solutions solve part of the problem of** minors protection but that it will be necessary to complement them with others, such as **blocking or filtering content** (as long as the user's age is not verified) or **tagging services, applications, sites or content** (to classify according to the age threshold from a technological point of view) so that the purpose of protecting the child is fulfilled. In this sense, **modifying or adapting** application stores, content access apps, or current browsers can greatly help integrate all the necessary elements.

D. MISCONCEPTIONS

It is common to find providers that manage age verification as if the ultimate purpose was to know the specific age of all users or which particular users are minors. However, this is not the case; the **purpose is to protect minors** from inappropriate content. This purpose can be fulfilled **without knowing the exact age of the users and without subjecting minors to verification processes**. With the **enabling approach** of age verification, it is adults who prove that they are "over the required age threshold" to access services, adult versions of apps, or specific content. Minors are thus **protected by default** without installing additional applications or tools, understanding the provider's information or undergoing new personal data processing. In short, **it is done proactively and without the need to take new risks**. To this end, verifying age, as mentioned above, and that the services and applications implement such protection by default is essential.

It is also common to think that any solution proposed to protect minors will involve **methods of avoidance or circumvention** and that, for this reason, no protection system should be deployed. For example, it is common to hear the argument that it is not worth the effort because minors will learn to use VPNs (Virtual Private Networks) to access inappropriate content or end up using an adult's proof of age or credential, which may even be falsified.

First, this is a mistake because current technology allows us to design and develop solutions that make it very difficult to get around them[14] (although possible, as with other types of protections in different application domains). Second, this same argument would apply to many protections for children in other contexts. However, society understands that the efforts made to protect most minors in most cases **involve a protection that reaches a high percentage of children,** and it is mandatory to deploy them.

[14] For example, if content filtering is carried out locally by browsers or content access apps installed on the user's device, circumventing the protection mechanisms may be complicated, especially when the minors' age is low.

VI. USE CASE 2: SAFE ENVIRONMENTS FOR CHILDHOOD

A. PRELIMINARY FRAMEWORK

Different participants in the Internet ecosystem are working to create safe environments for children. **However, there is no universal, concrete, and widely accepted definition of** what a safe environment or space for children on the Internet entails, nor of the requirements it must meet or its desirable properties. Unfortunately, this leads to important misunderstandings that different actors can exploit in a self-serving way.

There is currently a fairly widespread approach that is usually associated with this concept of the safe environment: the environments are the same for all users, **minors will be identified and, by default, also adults**, both will be **monitored in** their actions so that, when there is evidence of the exposure **to risk by** a minor, for example, the 5Cs mentioned in the Introduction section of this note, **corrective actions are taken**. All this is under **the criteria, supervision and surveillance** of the subjects by **Internet actors** whose legitimate interests, given their current business model, may collide directly with the protection of fundamental rights. In addition, using tools designed so that families, educators, regulators or authorities **cannot effectively exercise their different obligations**.

Generally, this **mistaken approach to a safe environment** is based on knowing who a child is and, in many cases, their specific age. Not only on the collection of the particular users' age (or their age range) but also in their **profiling**, including minors. In the latter case, to "improve the user experience" and make the services or applications more attractive or usable for users in different age ranges.

Marketing a service or application labelled as a "safe environment" can, in the worst case, allow **malicious actors** to attract, detect or locate children. In other words, this environment can produce the "fishing in a fishbowl" effect. Detection and location do not only imply knowing that a given account belongs to a child but also being able to associate an identity in the real world, a physical (geolocation) or digital address and having access to them to personalize messages, offers, etc. Even with the best will of the service or application provider, there is always the possibility that a member of the entity **will use it illegitimately** or that there is a **personal data breach** that exposes the child to third parties.

However, creating a safe environment should **seek, by design, to mitigate the threats** that may be generated on the fundamental rights of minors and all Internet users. It **is not enough to accumulate generic protections** to create a safe space; but these protections must be appropriate to the identified threats. Measures or tools to create safe environments must solve specific problems and **not generate new**, even more severe vulnerabilities. To this end, it is necessary to have a global vision of the measures adopted, which protect minors a priori and how they interact with each other.

Safe environments must be safe by design. I**t is not enough to include an additional layer of security** on top of the existing infrastructure; all actors have to evolve to incorporate the properties that make environments safe from the design. As mentioned in the previous use case, for example, app stores, apps themselves, or browsers. The Internet ecosystem **cannot be treated as a set of independent silos**. This requires **cooperation** between the parties involved in designing their solutions and **effective communication** between them in the face of identifying new threats to the minors' safety through an **appropriate governance framework.**

The measures protecting minors must allow the person with the duty of care to exercise their responsibilities. The **different obligations associated with creating** safe environments for minors on the Internet **cannot be delegated, nor should they be based on acts of faith**, especially on Internet actors whose interests are the monetization of users

and engagement, if not addiction, to their services and applications. In addition, they must be able to exercise them **by default**; that is, the lack of knowledge of those who have the duty to care for children of how specific measures or tools work does not pose a significant obstacle to protecting them.

The protection of fundamental rights does not only apply to the child but also involves **the protection of the rights of all Internet users**, in particular, the right to act physically and virtually, to non-discrimination, to education, expression and information, thought, conscience and religion, private and family life, etc., but, above all, the protection of physical integrity must be taken into account. It should be remembered that **minors are not the only group in a situation of vulnerability** due to certain practices of digital service and application providers.

B. LEGAL FOUNDATIONS

As mentioned above, **there is no definition of what a safe environment for minors is on the Internet**. But different regulatory frameworks include, from different perspectives, the protection that minors should receive in different contexts. In fact, they are the same as those analysed in use case 1, since this use case 2 can be considered an extension of 1 that takes into account other risks in addition to those produced exclusively by access to content. Additionally, the following should be considered.

DSA **recital 71**	The protection of minors is an important policy objective of the Union. An online platform can be considered to be accessible to minors when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes. Providers of online platforms used by minors should take appropriate and proportionate measures to protect minors, for example by designing their online interfaces or parts thereof with the highest level of privacy, safety and security for minors by default where appropriate or adopting standards for protection of minors, or participating in codes of conduct for protecting minors. They should consider best practices and available guidance, such as that provided by the communication of the Commission on A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+). Providers of online platforms should not present advertisements based on profiling using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor. In accordance with Regulation (EU) 2016/679, notably the principle of data minimisation as provided for in Article 5(1), point (c), thereof, this prohibition should not lead the provider of the online platform to maintain, acquire or process more personal data than it already has in order to assess if the recipient of the service is a minor. Thus, this obligation should not incentivize providers of online platforms to collect the age of the recipient of the service prior to their use. It should be without prejudice to Union law on protection of personal data.
DSA	Mitigation of risks

article 35	1. Providers of very large online platforms and of very large online search engines shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights. Such measures may include, where applicable: (a) adapting the design, features or functioning of their services, including their online interfaces; (b) adapting their terms and conditions and their enforcement; (c) adapting content moderation processes, including the speed and quality of processing notices related to specific types of illegal content and, where appropriate, the expeditious removal of, or the disabling of access to, the content notified, in particular in respect of illegal hate speech or cyber violence, as well as adapting any relevant decision-making processes and dedicated resources for content moderation; (d) testing and adapting their algorithmic systems, including their recommender systems; (e) adapting their advertising systems and adopting targeted measures aimed at limiting or adjusting the presentation of advertisements in association with the service they provide; (f) reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk; (g) initiating or adjusting cooperation with trusted flaggers in accordance with Article 22 and the implementation of the decisions of out-of-court dispute settlement bodies pursuant to Article 21; (h) initiating or adjusting cooperation with other providers of online platforms or of online search engines through the codes of conduct and the crisis protocols referred to in Articles 45 and 48 respectively; (i) taking awareness-raising measures and adapting their online interface in order to give recipients of the service more information; (j) taking targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate; (k) ensuring that an item of information, whether it constitutes a generated or manipulated image, audio or video that appreciably resembles existing persons, objects, places or other entities or events and falsely appears to a person to be authentic or truthful is distinguishable through prominent markings when presented on their online interfaces, and, in addition, providing an easy to use functionality which enables recipients of the service to indicate such information.

C. A FIRST APPROACH

Creating safe environments for children without requiring age verification from them is a **complex challenge**, but the **enabling, proactive, and default approach** mentioned above can help tremendously achieve this objective. The aim is **to balance accessibility and the protection of fundamental rights and freedoms** (including the child's best interests and privacy) to ensure that the Internet is an opportunity for all ages.

In this use case, minors **must be protected from** hateful, harmful or illegal content but also from **tools or functionalities** that place them in a vulnerable position for participating in hateful, harmful or illegal conduct, as well as **interactions with** other users that make them the object of hateful, harmful, illegal messages or problematic for different reasons. They must also be protected from cross-cutting risks that imply **over-exposure** or personal data processing with **new technologies** (artificial intelligence, Internet of Things, neurodata, biometric authentication). And, of course, from addictive patterns.

In the case of **adult services or applications**(model A in section IV), **there is no need** to design such safe environments for children, as children are not users and do not need to be protected. They are, by default, due to the age verification necessary to access these services and applications, which guarantees that you are over 18 years old if access has been achieved.

Regarding services or applications **for all audiences or mixed audiences**, there are two ways to offer safe environments for children, the B.1 and B.2 models already mentioned. For example, the B.1 model is followed by many streaming platforms, which allow the creation of safe-by-default accounts with specific protection, enabling them to be converted into safe spaces. If a service or application predicts having users of different ages, it can offer **different experiences according to age**, incorporating protection by design. This can be achieved with adult accounts, different apps for adults in app stores, etc. **Adults must always carry out age verification** to prove that they are adults when they want to open an adult account (verified with the service provider) or install the adult version of the app (verified in the store where they download the app). In this way, **minors are protected by default since they can only access safe-by-default accounts or apps**.

In all other cases, the B.2 model is applied, and all users are treated similarly, without differentiated experiences. The safe space must be safe by default and by design for all potential users, who may be of different ages. **Age-restricted content, features, and elements should only be accessible when the user is "over the required age threshold**" because an age verification process checks that their age is above the required age threshold in each case. A couple of good practices (5 and 6) examples have already been provided in section IV of this note. The functionalities and configurations available by default must always be safe and cannot be modified without an age verification process being carried out first.

In the two previous scenarios, in which a safe environment for minors is created, age verification could be complemented by some tools and processes such as:

- **Interlocutors' restriction:** These are specific methods and solutions offered to parents that limit the ability of minors to interact or communicate with other users so that it is limited to those who appear on allowlists or known contacts.
- **Parental involvement and parental control:** In this case, through other solutions that allow them to supervise and control the activity of their children's account without revealing the personal data of the child, configure safe searches or establish content or language filters.
- **Education for minors about online risks and responsible use of the Internet**: This includes recognizing suspicious behaviour and knowing how to report it on specific services and applications.

In addition, governments, NGOs, parents' associations and industry must collaborate, in a context of co-regulation, to create a safer digital environment for children by **identifying risks (and defining methodologies to do so), sharing best practices to manage them, developing codes of conduct**, etc.

D. MISCONCEPTIONS

Many current approaches are based on the interlocutor restriction and parental control mentioned above, as well as other types of tools that usually include:

- **Community-led moderation:** Trusted adult moderators (verified through thorough background checks) can monitor interactions to ensure they remain appropriate and child-friendly.
- **Automated moderation:** Automated systems can be set up to detect (before sharing) and remove (after sharing) inappropriate content or behaviour that is not adequate for children.
- **Peer-to-peer reporting methods:** Tools that allow minors to report suspicious behaviour that adult moderators can review.
- **Behavioural analysis:** Solutions based on machine learning or artificial intelligence that monitor play patterns, language use, or interaction styles to identify and flag behaviour (not users) inconsistent with that of a typical child.

However, these solutions **are not enough** to establish a safe environment, as they are based on reactive approaches (the child has already been exposed to risk) and do not protect minors by default. In addition, it would be necessary to analyse on a case-by-case basis whether they comply with the **data protection regulation** because some of these proposals are based on massive personal data processing or user profiling. Sometimes, automated decisions can generate serious legal effects and are also prone to bias. In short, they all may **violate the rights and freedoms of users**.

In this use case, there is also a widespread misconception that **a safe environment is created by allowing access only to children**. In this case, the age threshold is interpreted oppositely, as it is only "passed" when users are below the age threshold.

Assuming that an environment is safe because only minors are allowed access **is a mistake** since:

- As in the physical world, **a space is not safe just because only children are allowed to access it**. On the contrary, it is very likely that they do not have sufficient maturity or experience to face the risk situations that may arise or that they generate.
- This scenario **increases the risk of locating minors** and making them the target of commercial or malicious purposes (paedophile networks, etc.).
- Access to inappropriate content should be prevented by default for children, but what would prevent one from sharing it within one of these spaces? It is probably one of the moderation or reporting tools listed above, but a posteriori, following a **reactive approach that does not avoid risk exposure**.
- Protections **should not be applied reactively after** the child has already been exposed to the risk. They should be applied upfront, by default, and by design. Only in this way can we try to avoid or minimize the risk and its potential impact.
- The availability of the child to be contacted through the Internet must be **null by default** for anyone who does not belong to their trusted environment. It is not enough to trust that the rest of the users are all in the same age range.
    - A child may be **pushed or threatened** by an adult, directly or indirectly, to contact other children.

- The mixture of minors with very different ages could imply a risk. They should **not be treated as a homogeneous group**, nor should a direct association be made between age and maturity or stage of development.

- The protections that could be applied are, in many cases, **provided by third parties outside the child's trusted environment**, so those same third parties are a risk.
  - Determining a child's best interests is an obligation of parents and the other agents already mentioned in this note; it **cannot be left in the hands of technology companies** with legitimate commercial interests.

It should be noted that **no regulatory framework requires the creation of safe spaces in which all users are children.** The recommendations to make the Internet a safe space for children and age-aware can always be interpreted in the other sense: only users confirmed as adults can access certain content, have contact with other users without limitations, be exposed to certain functionalities or technologies, or modify certain settings.

VII. USE CASE 3: ONLINE CONSENT FOR PERSONAL DATA PROCESSING

A. PRELIMINARY FRAMEWORK

The current regulatory framework for data protection **allows the collection and processing of minors' personal data if certain conditions are met**. Consent may be one of the legal bases that legitimizes this processing of personal data (Article 6.1 and 8 of the GDPR, and 7 of the Spanish LOPDGDD[15]) or one of the conditions that may allow the prohibition on processing special categories of data to be lifted (Article 9.2 of the GDPR). In this context, **consent** is any free, specific, informed and unequivocal expression of will by which the data subject accepts, either by means of a declaration or a clear affirmative action, the processing of personal data concerning him/her, and in the case of minors under 14 years of age (in other European countries the age limit for consent may be different, but always **between the ages of 13 and 16**), that consent will have to be granted by those who hold their parental authority or guardianship.

In Spain, **minors between the ages of 14 and 18 may give consent for the use of their personal data themselves**, unless a specific rule requires the assistance of parents or guardians (Article 7.1 of the Spanish LOPDGDD). To this end, **the data controller must make reasonable efforts to verify** that consent was given or authorised by the holder of parental authority or guardianship over the child, taking into account the available technology.

The regulation does not specify what methods or mechanisms must be used by the controller to know if the user of an online service or application exceeds this age limit, nor how parental consent must be obtained when it is necessary or demonstrate that it has been obtained with due diligence.

B. LEGAL FOUNDATIONS

Some essential aspects in relation to consent for the processing of personal data in the case of minors are set out below:

GDPR **recital 38**	Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.
EDPB Guidelines 05/2020 on consent section 7.1	The words 'in particular' indicate that the specific protection is not confined to marketing or profiling but includes the wider 'collection of personal data with regard to children'.
GDPR **recital 58**	The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain

[15] (Spanish) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

	language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.
EDPB Guidelines 05/2020 on consent section 7.1	As mentioned in section 3.1. on informed consent, the information shall be understandable to the audience addressed by the controller, paying particular attention to the position of children. In order to obtain “informed consent” from a child, the controller must explain in language that is clear and plain for children how it intends to process the data it collects.61 If it is the parent that is supposed to consent, then a set of information may be required that allows adults to make an informed decision.
GDPR **considerando 75**	The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.
GDPR **article 8, Conditions applicable to child's consent in relation to information society services**	1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

	2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. 3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.
(SPANISH) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales **artículo 7, Consentimiento de los menores de edad**	1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento. 2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.
EDPB Guidelines 05/2020 on consent **section 7.1**	It is clear from the foregoing that Article 8 shall only apply when the following conditions are met: The processing is related to the offer of information society services directly to a child. The processing is based on consent. …. The ECJ held that information society services cover contracts and other services that are concluded or transmitted on-line. … In this respect, if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be 'offered directly to a child' and Article 8 will not apply. …. In particular, it should be noted that a controller providing a cross-border service cannot always rely on complying with only the law of the Member State in which it has its main establishment but may need to comply with the respective national laws of each Member State in which it offers the information society service(s). ….. When providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities.

	…. If the users state that they are over the age of digital consent then the controller can carry out appropriate checks to verify that this statement is true. … If the user states that he/she is below the age of digital consent then the controller can accept this statement without further checks, but will need to go on to obtain parental authorisation and verify that the person providing that consent is a holder of parental responsibility. …. Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor. If doubts arise, the controller should review their age verification mechanisms in a given case and consider whether alternative checks are required. … It is up to the controller to determine what measures are appropriate in a specific case. As a general rule, controllers should avoid verification solutions which themselves involve excessive collection of personal data. … controllers will also be expected to keep their processes and the available technology under constant review.
GDPR **article 12, Transparent information, communication and modalities for the exercise of the rights of the data subject**	1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.
EDPB Guidelines 05/2020 on consent section 7.1	After reaching the age of digital consent, the child will have the possibility to withdraw the consent himself, in line with Article 7(3). In accordance with the principles of fairness and accountability, the controller must inform the child about this possibility.
GDPR **article 40, Codes of conduct**	2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: …

	(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
EDPB Guidelines 05/2020 on consent section 7.1	Regarding the authorisation of a holder of parental responsibility, the GDPR does not specify practical ways to gather the parent's consent or to establish that someone is entitled to perform this action. Therefore, the EDPB recommends the adoption of a proportionate approach, in line with Article 8(2) GDPR and Article 5(1)(c) GDPR (data minimisation). A proportionate approach may be to focus on obtaining a limited amount of information, such as contact details of a parent or guardian. What is reasonable, both in terms of verifying that a user is old enough to provide their own consent, and in terms of verifying that a person providing consent on behalf of a child is a holder of parental responsibility, may depend upon the risks inherent in the processing as well as the available technology. In low-risk cases, verification of parental responsibility via email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information pursuant to Article 7(1) GDPR.68 Trusted third party verification services may offer solutions, which minimise the amount of personal data the controller has to process itself.

C. A FIRST APPROACH

Considering the rationale set out in the previous section, **whenever online consent is made** in a service or application for all audiences, **it must be verified that** the user providing it is "able to consent". In other words, they are over the age between 13 and 16 years established by law in their country (the +18 check of the use cases contemplated so far has gone from +14, for example, in Spain). When a user cannot verify this capacity, the personal data processing that requires consent can only be carried out after consent from those who hold parental authority or guardianship. If such consent is not given, the consequence could be providing **a service in a limited or different way** for these cases, not necessarily the user's inability to use the service.

In this case, services or applications for all audiences or mixed audiences, providers may offer different experiences depending on age (model B.1 of section IV), such as adult accounts, adult apps in the app stores, etc. **If the age restriction is made to concur with the age required for consent** (14 years in the case of Spain), the personal data processing whose legal basis is consent in safe-by-default versions can be avoided, or parental consent can always be requested for such processing by default. In the case of the adult versions, it is known that users can grant consent when necessary.

If the default protection (B.2 model) is implemented, all users are treated the same way, without differentiated access accounts or *apps*. Therefore, whenever personal data processing is based on consent, it is first necessary to **check whether the user is "able to consent"** by carrying out an age verification process.

In the case of adult services or applications that require verification that the user is over 18 years of age (model A), **it is already known that the user is of the appropriate**

age to consent to the processing of personal data, and Article 8 of the GDPR should not apply.

It is important to remember that before obtaining consent, the data controller must **provide at least basic information** on their identity, the purposes of the processing, the recipients of the data, and the exercise of rights (Article 7.1 of the GDPR). The request for consent shall be given in such a way that it is clearly distinguishable from other matters, in an intelligible and easily accessible manner, and using clear and straightforward language (Article 7.2 of the GDPR).

This means that **a service does not need to have messages adapted to children under 14 years old because they do not have to give consent**; it is granted by the adults who hold that responsibility. In turn, if a provider may have users over 14 years old, the information must also be adapted for them. Not **all users over 14 years of age are in the same circumstances for** reasons of education, culture, mental abilities, personal circumstances, urgency to access the service, etc. Trying to divide the type of messages for 14-18 and over 18 is a significant simplification.

In other words, when a service is for all audiences and the user's age or other circumstances are not known precisely, only that they are "able to consent", it must be guaranteed that the rights of all potential users are adequately protected, **by default and by design**.

While this note focuses on the use case relating to consent to processing personal data, a similar approach could be followed for risks associated with other consents or the signing of contracts, acceptance of terms, etc. It would be necessary, however, to make the appropriate nuances depending on the corresponding legal bases (the GDPR would not apply exclusively), age thresholds, etc.

It is also worth noting that age verification solutions solve part of the problem, but they will need to be supplemented with others, such as **parental consent or management of consent receipts**, to ensure compliance with all the obligations contained in the GDPR in relation to consent, specifically the consent of children.

D. MISCONCEPTIONS

In this use case, an **expansive interpretation** of the obligations involved in GDPR compliance is sometimes observed. It is not necessary to know the age of a service's users to comply with the regulation or to know which of these users are children in particular. It is only necessary to know that **they are over the minimum age to grant consent** in cases in which the service is offered to minors and in which it is also necessary to obtain that consent in order to process personal data.

It is also not necessary to verify the age of the minors in any case since the approach must be the opposite. The user who wishes to give consent must prove that he or she is capable of doing so.

Sometimes, the option of default protection is also criticized because it may imply an infantilization of all users. However, **the language involved in the request for consent and in the rest of the communications must be clear and straightforward for users over 14 years** old (in the Spanish case) when they can consent. This does not imply an infantilization of messages and can even indirectly benefit all users regardless of their age and circumstance. There is always the option, in addition, of letting the user choose, once their age above 14 years of age has been verified, between different options of messages, explanations, requests, etc., according to their degree of digital competence, maturity, etc.

VIII. USE CASE 4: AGE-APPROPRIATE DESIGN

A. PRELIMINARY FRAMEWORK

The term "age-appropriate design" **also does not have a universal, concrete and widely accepted definition**. In general, when this concept is used, it is associated with child-friendly design and usually refers to **services, applications, terms, conditions, policies, interfaces and user experience that are appropriate for children in general taking into account their rights and well-being** (including very specific rights, such as the right to play). And sometimes, the granularity of the term is increased to categorize children or adolescents according to their age.

It should be noted that different companies and organizations interact with children in an intentional or specific way while others do so in the course of their general activities, as they do with users of any other age. All of them must take into account use case 3 and what has already been explained regarding consent to the processing of personal data.

In any case, there is a certain **responsibility towards children to provide adequate, or at least, non-inadequate, services and applications**. But what does this responsibility entail? Who should assume it and to what extent? Because this use case must be clearly separated from the use case 2, which refers exclusively to safe environments and is therefore related to protection against risks associated with content, conduct, contact or cross-cutting. In this use case 4**, the risks are related to conduct, consumption, consent or contract and to other cross-cutting risks**. That is, with risks that may also affect the best interests of the child or their rights and freedoms, but in a different way. In general, without significant impacts on their physical and mental integrity.

It should be noted that the European Commission has recently formed a "Special group on the EU Code of conduct on age-appropriate design"[16] that has been working since the summer of 2023 on the EU Code of conduct on age-appropriate design (BIK Code). This code has not yet been made public, but other **child-friendly design codes have been,** such as the ICO[17], the first published, or the California Age Appropriate Design Code[18] (which is awaiting a court decision to begin to be applied[19]). Different countries are currently working on new drafts of which some details have already been shared.

Also interesting for this use case is the *2089-2021: IEEE Standard for an Age Appropriate Digital Services Framework*[20] based on the previous work of the 5Rights organization, which focuses on the **processes that organizations must carry out to make their services and applications suitable for children**. There is also a Workshop Agreement of September 2023 in relation to this standard at European level, through CEN and CENELEC (CWA 18016[21]).

B. LEGAL FOUNDATIONS

The concept of child-friendly design is transversal, since the rights of children, their well-being and the protection of their best interests appear in many and very heterogeneous regulations. Mentions to appropriate design can be found in European regulation for:

- Data protection (already discussed in the previous use cases).

[16] https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design
[17] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/
[18] https://californiaaadc.com/
[19] https://natlawreview.com/article/california-age-appropriate-design-code-act-enjoined
[20] https://ieeexplore.ieee.org/document/9627644
[21] https://www.cencenelec.eu/news-and-events/news/2023/eninthespotlight/2023-09-14-cwa-18016-children-protection-online/

- Consumer protection.
- Security and protection of physical and sexual integrity and against abuse.
- Digital services, products and markets.
- Education.
- Health.
- Equality.

The fundamental difference with the three use cases already discussed in this note is that child- or age-appropriate design is usually not a legal obligation, but a recommendation or a desirable but optional element.

C. A FIRST APPROACH

Following the same reasoning as in the use cases above, **adult services or apps do not need to worry about offering a child-friendly design**. Services or applications for all audiences or mixed audiences can consider doing so, and two scenarios are distinguished.

When separated by age (model B.1), the version for the children's experience should conform, by default, to the different recommendations contained in the appropriate design codes that are applicable. This is not the case with the adult version. In this case, **the age limit is not set in any European regulation** but in the already mentioned codes and in the obligations or recommendations they contain.

In the case of default protection (model B.2), all users are treated the same way because their age is unknown, nor if they are over a certain age. The standards of the code must be applied to all users so that **minors are constantly exposed to a design suitable for them**. This ensures that their needs are respected and their best interests are protected. **Adults who verify their age can modify this interface or default settings**. This approach can benefit users with less digital competence, specific disabilities or older people, to mention just a few examples.

About the latter, a good practice, in general, is **to avoid relating maturity or digital competence with age**. All users (not just children) should have the option to voluntarily access different design versions of the interfaces of the services and applications they use according to their needs and preferences. This **adaptive design** does not necessarily have to be based on age verification processes but on giving users options to freely choose the ones they believe are most suitable, useful or beneficial. **The browsers or applications that access the different services can provide significant support in everything related to this adaptive design**. The user would not have to make this selection on a case-by-case basis and on each occasion but that their decisions can be remembered or automated according to specific configurations or preferences.

D. MISCONCEPTIONS

In the case of child-friendly designs, there are significant misunderstandings regarding **services and applications classified by age range**.

In short, the first is the **need to know the minor's age and confuse it with the degree of maturity**, which varies between genders and educational and cultural situations, for example. As already explained, with the enabling, proactive and default approach of age verification, it is adults who, in some cases, will have to verify their age to access a suitable or comfortable design for them and not the other way around. Also, only when they want this

type of adaptation since it could happen that due to their degree of maturity or other circumstances, they prefer the interface that by default is considered suitable for minors (this only with model B.2, with models A and B.1 they will have a default interface different from the one appropriate for children).

The second is that an Internet provider predetermines a child's degree of maturity based on their age or age range, and **it is not the family, or even the child**, who can choose which design they want to use, taking into account their personal circumstances. Providers should not impose restrictions on how minors use the Internet based on their particular criteria.

The third is the lack of specificity or standardization of the term "appropriate design." We must ask ourselves**, what is appropriate for what?** Since one answer may be that it is more persuasive or addictive for children, turning this type of design into **a deceptive pattern that should be avoided due to the risks involved**.

IX. APPLICATION OF THE DECALOGUE PROPOSED BY THE AEPD

As previously mentioned in this note, the AEPD published in December 2023 its "Decalogue of principles: Age verification and protection of minors from inappropriate content". This decalogue was proposed to facilitate compliance with the GDPR and the safeguard of the **best interests of the child** in scenarios where the purpose was to protect minors from **inappropriate content**. Content in the broadest sense of the word, since it can also be services, functionalities or products. In other words, it was essentially focused on use case 1 of this technical note.

However, as has been analysed in the previous sections, age verification solutions can be used in **other scenarios different from this one**, so one may ask if the proposed decalogue of principles can be applied directly to these use cases that are not exclusively related to the protection from inappropriate content but from other types of risks.

The answer is yes, since the approach to using age verification as a fundamental solution for minors' protection is the same in all use cases: it should be used **only when necessary, minimising the data processed** (it is not necessary to know the date of birth or the exact age, only that an age threshold is exceeded), putting the **burden of proof on the user who exceeds the age threshold** (age verification is always an enabler) and **respecting the principles and requirements set out in the GDPR**. The language in which these principles are expressed would simply have to **be generalised** so that they are applicable to all use cases:

- **Principle 1:** Age verification should not make it possible to identify, track or locate minors over the Internet.
- **Principle 2:** Age verification should enable persons of the appropriate age to prove their status as a person who "exceeds the required age threshold", and not conversely, to prove their status as a "minor" or "does not exceed the required age threshold".
- **Principle 3:** Evidence of exceeding the required age threshold should be anonymous to Internet service providers and third parties.
- **Principle 4:** The obligation to prove the status of a person who "exceeds the required age threshold" should be limited only to processing in which such accreditation is necessary.
- **Principle 5:** Age verification must meet the requirements of accuracy, effectiveness and data minimisation. For the latter, it should categorize whether the person "exceeds the required age threshold" or equivalent.
- **Principle 6:** Age verification should not make it possible to profile persons based on their Internet browsing.
- **Principle 7:** Age verification should not make it possible to link a person's activity across different Internet services.
- **Principle 8:** Any solution for age verification should ensure that parental rights are exercised by parents when the use case requires it.
- **Principle 9:** Any solution for age verification must respect the fundamental rights of all persons in their access to the Internet.
- **Principle 10:** Any solution for age verification should have a defined governance framework.

X. CONCLUSIONS

A safe Internet by default means **guaranteeing minors their rights and freedoms in the digital ecosystem** by minimising the risks associated with harmful content, contact with other people, induction to harmful behaviour, contracting products and services or lack of control over their own personal data, to mention just a few examples.

Age verification solutions are an **essential tool** to achieve this safe Internet by default and can help manage the risks associated with the 5Cs: Content, Contact, Conduct, Consumer (consent or contract) and Cross-cutting. This is reflected in different **national and European regulations that impose obligations** on Internet actors. However, it should be noted that age verification solutions are not enough to protect minors online. Internet services and the tools that allow access to them (such as apps offered in stores or browsers) must **properly integrate age checks with other solutions** and tools to protect children and all citizens' rights.

This note has identified **different models** to incorporate age verification on Internet services and applications **from the design and by default**. It has analysed them in four distinct use cases: protection against inappropriate content, safe environments for children, online consent for the processing of personal data and age-appropriate design. **Each use case analysed is subject to the GDPR for processing personal data and other regulatory frameworks that must be carefully examined** to ensure that the processing of personal data during the age verification process is **lawful**.

There are **misunderstandings, errors, ambiguities, and misrepresentations** about minors' protection on the Internet, particularly regarding its requirements, desirable properties, and implications. Some of the most dangerous misconceptions are those **related to "safe environments", "accounts for minors", or the design "appropriate for children".** In many cases, it is proposed to know which **specific users are minors** to configure and monitor their activity while connected. This poses a risk since the minor is located and easily accessible to third-party services (authorised or unauthorised) or explicitly malicious, creating the effect of **"fishing in a fishbowl"**.

A common excuse for knowing which specific users are minors is that the information for decision-making must be adapted to a language they can understand, for example, in the case of terms of service. However, the decision-making to consent to the processing of personal data, to contract or consent to contact with other users is an obligation, the duty of care, which legally falls on those who hold parental authority or guardianship. **It is not necessary to adapt the language for children to make decisions that, according to their age, do not even correspond to them**.

Another excuse used to locate children is the adaptation of digital environments or designs to their age. However, this means that minors must be in Internet environments that offer the same characteristics and functionalities to all users between 5 and 14/16/18 years old or that greater granularity is required to determine their age. These users are forced to adapt to the "average" or standards a provider defines. Again, there is a risk of keeping minors in separate "playpen" type spaces. In addition, these approaches may seek **to legitimize the processing of the minor's data, or all users,** and hide purposes of more precise profiling concerning deceptive and addictive patterns, loyalty, contracting, consumption or monetisation of personal data. In addition, in many cases, they involve the use of **new identity management schemes on the Internet**, either specific to minors or to all users, which collect personal data outside the guarantees of personal identity developed in national or European regulation, dependent on service providers (sometimes located outside the EU) and with no availability guarantees. Furthermore, what could be more worrying is that **they turn people's identity, a right, into a service**.

Another widespread mistake is the one that aims to offer a safe Internet by default based exclusively on **reactive** strategies: allowing the processing of children's personal data, exposing them to risks and, in the best of cases, reacting when it is detected that damage is being caused. This involves **exposing the minor** to, for example, any user being able to contact them, subjecting all users to monitoring and profiling techniques, accumulating evidence of harassment or paedophilia, applying criteria established by the service provider, and finally, acting. This strategy requires that harm is caused to minors and, in addition, that there is an intrusive and systematic intervention in the privacy of all users so that **the processing of personal data involved is not effective or fair**.

This note explains how to achieve a safe Internet by default with **a paradigm shift that** rejects all these misunderstandings. The approach to risk management for minors must always be **proactive**, focused on prevention, and avoid or minimise impacts and damages, not reacting once they have occurred. **Age verification should be an enabler**, verifying that users are above the age threshold required to pass, perform an action, or access an item online. In this way, it is avoided to involve minors in age verification (with the consequent processing of personal data); they are **protected by default**. Therefore, the minor must not prove they are minors nor expose their nature so that content, contacts, behaviours or contracts are "blocked". On the contrary, this paradigm gives family members and guardians back the ability to exercise their **duty of care**, shifting the burden of proof to users who can take risks and are willing to do so.

A safe Internet by default can be achieved by applying the **decalogue** of principles proposed by the AEPD for age verification in all the use cases analysed and in others that may arise related to the protection of children from the risks associated with the 5 Cs. **Age verification or knowing the age of users is not the purpose** or objective in itself; the purpose of any data processing within the framework of the four use cases described is the protection of children.

The **design decisions** of these solutions must always be based on rigorous processes **based on both technical and scientific evidence** (for example, concerning the physical and mental integrity of children) and **risk management** for children's rights and the protection of children's data and users in general, and not on intuitions, fashions or beliefs. Therefore, decisions for the management of these risks for minors should be based on a **Children's Rights Impact Assessment (CRIA)** and the processing that is implemented for this, in particular age verification processing, given the **high risk** to the rights and freedoms of individuals, on a **Data Protection Impact Assessment (DPIA)** to be carried out by the controller of such personal data.

It is necessary to comply with the principle of **data minimisation, among others, to pass this DPIA.** In any use cases analysed, age verification does not need to verify a specific age or date of birth; only the user must be above the necessary age threshold. In addition, all reasonable measures must be taken to ensure that the personal data processed in age verification processes are **accurate regarding the purposes** for which they are processed, i.e. a **sufficient level of certainty** must be ensured when verifying that a user is above the required age threshold, as this is what allows the purpose of the processing to be fulfilled, protect the minor from the risks already mentioned. This ensures the **effectiveness** of the processing of personal data that is carried out to verify age.

Including a cybersecurity layer on top of the Internet ecosystem is not enough. Internet service providers must evolve and **implement data protection principles by design and by default**.

The Internet ecosystem **cannot be treated as a set of independent silos**. The **cooperation of those within the Internet ecosystem involved in the design of the solutions is essential to achieve a paradigm shift** in minors' protection. Furthermore,

effective communication between them is required in the face of identifying new threats through a **governance framework.** Those involved are providers, manufacturers, intermediaries and other Internet operators, as well as data protection and consumer authorities and those competent in market regulation, especially of products and services offered on the Internet. Also, governmental and non-governmental organisations having the education and protection of minors as their purpose, both Spanish and European. And, of course, those responsible for processing personal data that consume or use such products and services offered on the Internet and those who hold parental authority or guardianship of the children.

XI. BIBLIOGRAPHY

(Spanish) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE núm. 294, de 06/12/2018. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

(Spanish) Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual. BOE núm. 163, de 08/07/2022. https://www.boe.es/buscar/act.php?id=BOE-A-2022-11311

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/eli/reg/2016/679/oj

Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities. https://eur-lex.europa.eu/eli/dir/2018/1808/oj

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). https://eur-lex.europa.eu/eli/reg/2022/2065/oj

5Rights Foundation. (2024, March). The best interests of the child in the digital environment. https://5rightsfoundation.com/uploads/dfc-report-best-interests-of-the-child.pdf

5Rights Foundation. (2024, April). Enforcing the online safety act for children: Ambitions for the children's safety code of practice. https://5rightsfoundation.com/uploads/enforcing-the-online-safety-act-for-children-children-s-coalition.pdf

Cannataci, J. A. (2021). Artificial intelligence and privacy, and children's privacy: Report of the Special Rapporteur on the right to privacy. A/HRC/46/37. United Nations Human Rights Office of the High Commissioner. https://www.ohchr.org/en/documents/thematic-reports/ahrc4637-artificial-intelligence-and-privacy-and-childrens-privacy

Digital Trust & Safety Partnership. (2023, September). Age Assurance Guiding Principles and Best Practices. https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf

European Parliamentary Research Service. (2023, February). Online age verification methods for children. https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf

eSafety Commissioner. (2023, December). Phase 1 Industry Codes (Class 1A and Class 1B Material) Regulatory Guidance. Australian Government. https://www.esafety.gov.au/sites/default/files/2023-12/Phase-1-Industry-Codes-%28Class-1A-and-Class-1B-Material%29-Regulatory-Guidance.pdf

Mukherjee, S., Pothong, K., & Livingstone, S. (2021, March). Child Rights Impact Assessment: A tool to realise child rights in the digital environment. Digital Futures Comission. https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf

Sas, M., & Mühlberg, J.T. (2024, February). Trustworthy age assurance? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective. The Greens/EFA in the European Parliament. https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance

Shaffique, M. R., & van der Hof, S. (2024, February). Research report: Mapping age assurance typologies and requirements. Better Internet for Kids (BIK) project. https://op.europa.eu/en/publication-detail/-/publication/215f6c72-fe04-11ee-a251-01aa75ed71a1/language-en/format-PDF/source-search

UN Committee on the Rights of the Child. (2021, March). General comment No. 25 (2021) on children's rights in relation to the digital environment. CRC/C/GC/25. United Nations Human Rights Office of the High Commissioner. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

UNESCO. (2023, April). Safeguarding freedom of expression and access to information: guidelines for a multistakeholder approach in the context of regulating digital platforms. https://unesdoc.unesco.org/ark:/48223/pf0000384031

van der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., & Liefaard, T. (2020). The child's right to protection against economic exploitation in the digital world. The International Journal of Children's Rights, 28(4), 833-859. https://brill.com/view/journals/chil/28/4/article-p833_833.xml