TECHNICAL NOTE

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

October 2024

INDEX

I. EXECUTIVE OVERVIEW 3

II. INTRODUCTION 4

III. BACKGROUND AND CONTEXT 7

A. Obligations in the Internet ecosystem 7
B. Security by default and by design 7
C. Age verification 9
D. Systemic risks 10
E. Categorising risks to children on the Internet 11

IV. MODELS FOR AGE VERIFICATION 15

A. Services and applications for adults 15
B. Services and applications for all or mixed audiences 17

V. USE CASE 1: PROTECTION AGAINST INAPPROPRIATE CONTENT 23

A. Preliminary framework 23
B. Legal basis 23
C. A first approach 25
D. Misunderstandings 25

VI. USE CASE 2: SAFE ENVIRONMENTS FOR CHILDREN 27

A. Preliminary framework 27
B. Legal basis 28
C. A first approach 30
D. Misunderstanding Equivocal 31

VII. USE CASE 3: ONLINE CONSENT TO DATA PROCESSING STAFF 34

A. Preliminary framework 34
B. Legal basis 34
C. A first approximation 38
D. Misunderstandings 40

VIII. USE CASE 4: AGE APPROPRIATE DESIGN 41

A. Preliminary framework 41
B. Legal basis 42
C. A first approximation 42
D. Misunderstandings 43

IX. IMPLEMENTATION OF THE DECALOGUE PROPOSED BY EPPD 44

X. CONCLUSIONS 45

XI. BIBLIOGRAPHY 48

I. EXECUTIVE OVERVIEW

This AEPD technical note demonstrates that **it is possible to effectively protect children and adolescents (children and adolescents) on the Internet without systematic surveillance or invasion of the privacy of all users**, and without exposing children and adolescents to being located and exposed to new risks. This requires a **change in the paradigm** used so far to protect children: instead of using current reactive strategies, it is proposed to achieve real and effective protection of children by applying **data protection** principles **by default**. This change of approach when designing the processing of personal data carried out on the Internet makes it possible to configure a safe space by default for children that guarantees that children can **enjoy their rights and freedoms in the digital environment.**

This note analyses **four different cases of use** and recommends good practices to protect children and adolescents, and by extension all vulnerable groups, in their access to the Internet from risks related to access to content, contact with people who may put them at risk, contracting products and services, monetisation of their personal data, inducing addictive behaviour that affects their physical or mental integrity, and other cross-cutting aspects. **All these risks have as their cause or effect the processing of personal data of minors**.

Reactive strategies employed so far are based on allowing children to be exposed to such risks and, ideally, reacting when harm or impact is already detected. Protection has also sometimes been proposed based on ISPs knowing **which user is a child**, for example, to enable the creation of specific spaces or accounts for children. These strategies **require an intrusive intervention in the form of surveillance or profiling** that systematically violates the privacy of all users: they allow **the child** to **be located and easily accessible** to any malicious actor, they may seek to **legitimise new processing of children's personal data**, they adapt messages to make decisions that, in many cases, do not correspond to them, or they may **hide profiling purposes** in relation to deceptive or addictive patterns, loyalty, recruitment, consumption or monetisation of personal data.

All of these risks can be avoided by enforcing the right of children and adolescents, and other vulnerable groups, to a **safe Internet by default**. Secure beyond cybersecurity, in the sense of preventing any harm to children's best interests and fundamental rights due to the processing of their personal data, so that children, families and other users are in control of their own data.

Age verification is one of the tools that enables the design of this secure Internet by default, and the AEPD's proposal is that this age verification should be an **enabler** for accessing any element that implies a risk, assumable for people with sufficient maturity and information, or for making decisions when they assume parental authority or guardianship of a child. Furthermore, keeping **the burden of proof on the age-appropriate user, 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 complies with all the principles and requirements set out in the GDPR, in addition to the adaptation of Internet services and integration with other solutions so that it is effective, does not generate new risks, does not allow children to be traced and its use does not entail any loss of rights or freedoms.

II. INTRODUCTION

The internet offers educational, social or creative **opportunities** for children and adolescents. However, within the framework of the processing of their personal data, **new risks** associated with inappropriate content, cyber-bullying, exploitation, addictions or consent to certain activities or operations materialise on the Internet. Other risks affecting children and young people are those that involve considering them as passive subjects who can be **targeted, manipulated or turned into** long-term captive **customers**, or treated as **monetisable products** through their "datification". Protecting **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 in relation to the processing of personal data in general, and **with greater guarantees when it comes to children's personal data**. These entail specific compliance obligations that legitimise processing and manage risks to the rights and freedoms of children and all internet users.

The strategy followed **so far** to protect children online by most digital product providers has been **reactive**. That is, maintaining a design of services that allow **children to be exposed to such risks** through the processing of their personal data and, at best, reacting when it is detected that harm or impact is already occurring. This involves exposing the child to, for example, being contacted by any user; subjecting all users to surveillance and profiling techniques; accumulating evidence of harassment, *grooming*, paedophilia or other; applying criteria set by the provider; and finally taking action. This type of strategy requires evidence of harm to the child in order for protective measures to be triggered. Other strategies are based on **enabling ISPs to** know **who a child is**, or even what age they are. For example, when offering specific spaces or accounts for minors. In this way, the provider aims to configure and monitor the activity of the child during the use of their service or tailor messages to make decisions (which, in many cases, are not theirs to make).

The implementation of these strategies requires **intrusive intervention by Internet services in the form of surveillance or profiling** that systematically violates the privacy of all users. Moreover, they imply **having the child located and easily accessible** to third party services or, directly, malicious actors. This strategy **may seek to legitimise a massive processing of personal data of children and all users.** In addition, they may **hide purposes of profiling** in relation to deceptive or addictive patterns, loyalty, recruitment, consumption or monetisation of personal data. In many cases, they also aim to create **new digital identity schemes**, with identity as a service rather than a right. And it is these schemes, initially applied to children, that will be extended in the future, given that users who are children now will become adult users later on.

These risks can be avoided by enforcing the right of children and other vulnerable groups to a **safe internet by default**. It should be made clear that safety means much more than cybersecurity. Security means preventing harm to children's best interests and fundamental rights from the **processing of their personal data**. Not only must their personal data be protected from unauthorised processing, loss, destruction or damage, but **children** must **also be protected from risks that result from "authorised" personal data processing** and that cause or result in, for example, harm to their physical and mental integrity. Also

means giving **decision-making power over their own data** back to the child, and to those with parental or guardianship rights, which means being able to decide the extent to which the child is exposed to potentially harmful contacts, contracts, conduct and content.

A secure internet by default must be built **by design**, and following the principle of minimisation, as the processing of children's personal data, its location and accessibility, are some of the main causes of risk. To this end, it is not enough to include an additional layer of security on top of internet services as they are currently implemented, but **internet service providers have an obligation** to evolve to **implement data protection principles by design and by default**.

Age verification is one of the tools that enables the design of a safe Internet by default, although it is not the only one, nor can it alone provide a solution to all the challenges that this design implies. Age verification should be understood as an **enabler** to access any element that implies a risk, assumable for people with sufficient maturity and information, or to make decisions when assuming parental authority or guardianship of a minor. In this way, **the child does not have to prove that he or she is a minor**, nor does he or she have **to** expose his or her nature in order to block content, contacts, contracts or functionalities, or to receive information in order to make decisions that do not correspond to him or her. On the contrary, this **proactive** approach returns to family members and guardians the ability to exercise their duty of care, and **shifts "the burden of proof" of exceeding an age threshold for exposure to risk**, and the willingness to do so, to the adult, as established in Article 8 of the GDPR and Article 7 of the LOPDGDD. In order to be effective, moreover, it must be done **by default**.

With a secure internet by default, a child's child status or age is not exposed or processed. The processing of children's personal data, including their status as minors, is not necessary, proportionate and, in many cases, not fair. **The burden of proof of exceeding the age threshold necessary to engage in a given activity on the Internet rests with the age-appropriate user. And it will be up to an adult user to select those elements (with the associated risks) that are appropriate to the maturity level of the child under his or her guardianship**. The type of content that a child 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 with parental authority or guardianship, who are the ones who have to 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 curtailing the rights and freedoms of all users. In particular, age verification **should 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 islands**. Implementing a paradigm shift in child protection requires not only **cooperation** between actors (providers, manufacturers, intermediaries, etc.) in designing their solutions, but also **effective communication** between them and with the rest of society in identifying new threats through a **governance framework.**

Therefore, this document is addressed to **Internet providers, manufacturers, intermediaries and other Internet operators**, as well as to **data protection, consumer and market regulation authorities**, especially for products and services offered on the Internet, and to **governmental and non-governmental organisations** whose purpose is the education and protection of minors, both in the field of education and in the field of child protection.

Spanish as well as European. Of course, it is also addressed to **personal data controllers** who consume or use such products and services offered on the Internet and to those **who have parental authority or guardianship** over children.

III. BACKGROUND AND CONTEXT

A. OBLIGATIONS IN THE INTERNET ECOSYSTEM

Different actors such as parents, educators, governments, regulators, judicial authorities or law enforcement authorities **must assume their corresponding obligations** to ensure that children can take advantage of the opportunities offered by the digital space while being **adequately protected from the risks** it poses. In particular, members of the technology industry must assume their obligations in child protection in a way that complies with existing regulation, in particular **data protection compliance** either as data controllers or data processors, and be more ambitious by incorporating proactive tools and adapting processes that allow the aforementioned actors to exercise their different responsibilities. Furthermore, it should be borne in mind that **Article 28 of the Digital Services Regulation** states that online platforms that may be used by minors 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 for the various players in the Internet ecosystem (manufacturers, other providers, intermediaries, etc.), should provide **an environment that is safe by default for children**, without arrogating to themselves roles that belong to parents, educators, governments, regulators, judicial authorities or law enforcement authorities. Child protection will be at risk if they are prevented from exercising their duties in the supervision, care and education of children. **Their various responsibilities cannot be delegated**, nor should they be based on "leaps of faith", especially by internet actors whose interests, given their current business model, may directly collide with the **protection of the fundamental rights** of all users.

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

B. SECURITY BY DEFAULT AND BY DESIGN

Until now, the **prevention** of risks to children on the Internet has been left mainly in the hands of children themselves and their **parents and educators**. **Providers** and other actors in the digital ecosystem have focused on developing **reactive strategies** in which, once children are exposed to risks and even once harm or impacts have occurred, they act accordingly. A clear example is the possibility (even the encouragement) that anyone can initiate contact with a child through a service or platform without, by default, the decision of who can make this contact being in the hands of those with parental authority or guardianship. Only when there is evidence of any kind of harassment, following the criteria of the service provider itself, are alert mechanisms triggered.

This approach poses **a risk to the best interests of the child and to his or her fundamental rights**. But also for the **fundamental rights of other internet users**, as it focuses on **the monitoring and profiling** carried out by the

service providers to detect risk situations and their potential impacts with criteria established by themselves. It implies processing of personal data that is not necessary and **does not comply with the minimisation principle**. This approach means that the reaction, if it occurs at all, takes place after potentially irreversible damage has already occurred, and therefore does not pass a necessity analysis. The treatment is unsuitable as it does not fulfil its objective effectively.

Reactive measures have been justified in the past because digital products have been designed to make it difficult or impossible for parents, educators, governments, regulators, judicial authorities or enforcement authorities to exercise their obligations in relation to child protection. All of these digital products **facilitate by design, or even encourage, children to become users**. Once they are users, it is up to the providers of such products to carry out the necessary processing to deploy such reactive measures. This could be **a breach of the principle of fairness**. Fairness is a general principle that requires that personal data should not be processed in a way that is unjustifiably prejudicial, unlawfully discriminatory, unexpected or misleading to the data subject.[1].

Taking the physical world as an example, to guarantee children's right 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 different duties and establish, in each case, *a priori* measures to avoid the main elements of risk.

But 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 aforementioned actors (parents, educators, governments, regulators, judicial authorities, control authorities) in order to achieve it. This requires a **holistic view** of the best interests of minors and the protection of their fundamental rights, i.e. a safe Internet by default cannot be limited to specific aspects (access to inappropriate content, grooming, addiction, etc.), nor considered in a disconnected way, but **all rights** must be considered **in a unified way, without establishing any hierarchy or priority between them**.

It should also be borne in mind that the safety of children on the Internet is directly related to the concept of ***safety* or protection**, i.e., it must be guaranteed that, under the guise of biased or misunderstood security, the best interests of children are not harmed and that their fundamental rights are not violated. And not so much with the concept of *security* or security (cybersecurity), i.e. the guarantee that the information linked to the child's activity is subject to adequate measures that reduce the risk of accidental loss, destruction or damage. Although **security is an important factor** in achieving protection, the latter **cannot be reduced** to the former, which 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 children, even with serious impacts on their rights and freedoms.

[1] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020: from https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

C. AGE VERIFICATION

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

Age verification solutions are those that **determine whether a user is over the minimum age required to pass an online *age gate***. For example, if a user exceeds the 18 years required to play a video game that is classified as violent or to configure a messaging *app* so that messages from any other user can be received 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.

The GDPR requires compliance with the principle of accuracy of data with respect to the purposes for which they are processed (Article 5(1)(d) of the GDPR). Age verification, insofar as it may limit fundamental rights, must be accurate in terms of its suitability to fulfil its purpose: to enable access to certain elements of the internet that pose a risk to children. This does not mean that it is always necessary for providers of digital products to process the date of birth of Internet users. **Collecting the date of birth or the precise age** of Internet users, when it is not necessary, is contrary to the principle of minimisation. In most use cases it will be sufficient to know whether the user **is above an age threshold** or, in case of relying on trusted third parties through *tokenised* architectures, simply whether he/she is able to access the Internet.[2]simply whether he/she is able to access the requested element with an "over the required age threshold", "YES", "OK", etc.

The approach to the application of age verification should always be one of **empowerment**, i.e. aimed at demonstrating that the age threshold is exceeded and that the operation being requested can therefore be carried out. In this way, the risk for minors is limited, data minimisation is applied, and the processing is proportional, as the processing of personal data of children and adolescents to obtain specific accreditations or certificates, install applications, etc. is avoided. Digital products should protect children **by default and by design**, preventing them from running risks, not waiting until they are already 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 online protection, as it is one of the tools with the greatest potential for child online protection. But, at the same time, with more **privacy and data protection implications**. Indeed, as age verification is likely, by its nature, scope, context or purpose, to entail a high risk to the rights and freedoms of individuals, the controller of personal data associated with age verification should, prior to the processing, carry out **an assessment of the impact of the processing on the protection of personal data**.

[2] In this type of technological architectures a trusted third party provider specialised in performing age verification performs the appropriate checks with the user, so that the application or service provider only receives a token or credential that proves that the user is above the required age threshold, no other information.

D. SYSTEMIC RISKS

In relation to these implications for rights and freedoms and the concept of risk, it must also be avoided that age verification solutions can have a **really significant impact on society**, the economy or security because of their wide influence or their ability to affect a large number of users.[3]. Such risks could occur if the provider of a verification solution is granted monopoly power, or the ability to profile a significant number of Internet users or if a breach of its security could affect sensitive data of that significant number of users.

It should be borne in mind that not only risks to the best interests of the child and to the rights and freedoms of all citizens must be avoided, but also **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 harm to individuals on a large scale or to systems essential to the governance and proper functioning of society**.

According to 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 Regulation) there are **four categories of systemic risks** (recital 80). Two of them are very closely related to the processing of personal data in age verification solutions.

The second category identified in the Regulation (recital 81) concerns the **actual or foreseeable effects of the service on the exercise of fundamental rights** as protected by the Charter. If age verification solutions are not properly designed and implemented, many of these rights may be infringed, including freedom of expression and information, the right to privacy, the right to data protection or the right to non-discrimination.

In particular, and in relation to the right to data protection, child protection is sometimes used as a **justification for the mass collection of data on children and other Internet users**: mass profiling, categorisation of content and users, automated evaluations or decisions, etc. Age verification solutions are in some cases proposed as solutions for **managing the digital identity** of Internet users. This identity, provided and managed as a service rather than as a right, **is not under the control of the users themselves**, but depends on the criteria and interests of a provider who can, at its discretion, remove this identity or limit the ability of individuals to act.

The creation of a safe Internet by default for children cannot, under any circumstances, be an alibi for such massive processing of personal data that does not comply with the principles of fairness, transparency or data minimisation and would violate different rights and freedoms. This risk would be systemic given its potential scale and scope.

Furthermore, it should be borne in mind that an age verification solution that would corner a large part of the market could lead to **a timely unavailability of access to content, services, contracts**, etc. affecting different rights and freedoms, but also the resilience of the digital infrastructure and the economy.

[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 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 on public security**. It should be borne in mind that, due to their scale and level of intermediation in information flows, certain services and applications have become public spaces with a central role in facilitating public debate, access to information or economic transactions, to mention a few examples. The potential harm, for individual users but also for society, of poorly designed and implemented age verification solutions in terms of their appropriateness is enormous (errors, biases, exclusion, etc.). Again, the creation of a safe Internet by default for children **cannot, under any circumstances, be an alibi for limiting access** to these services and applications in breach of the principles of lawfulness, fairness or accuracy and which would violate various rights and freedoms. This risk would also be systemic given its potential scale and scope.

While these two categories of systemic risks are the ones that age verification solutions can cause if they are not designed or implemented properly, there is a further reflection: **not performing age verification at all, or doing it in a way that is not suitable, can also entail systemic risks**. Indeed, the fourth category of risks identified by the DSA stems from the **design, operation or use, through manipulation, of very large online platforms and very large online search engines, with an actual or foreseeable negative impact on the protection of public health, minors and serious negative consequences for a person's physical and mental well-being, or on gender-based violence**. As set out in this technical note, age verification does not completely prevent these risks to the physical and mental well-being of minors, but it is a fundamental tool for their protection. Thus, in certain cases, not carrying out age verification at all, or carrying it out in a way that does not fulfil its function, may also pose a systemic risk, in particular when such a system allows for the identification and detection of children on the internet.

E. CATEGORISING RISKS TO CHILDREN ON THE INTERNET

To understand how age verification can help protect minors online, it is first necessary to understand what exactly minors need to be protected from. This note uses the OECD classification[4]so that five categories of risk, the so-called five Cs, are taken into account:

1. **Content:** Hateful content (race, gender, religion, sexual orientation, etc.), harmful content (pornography, extreme violence, substance abuse, extremism, eating disorders, etc.), illegal content (sexual abuse, terrorism, etc.) and misinformation can have an impact on children's mental health and emotional development.
2. **Behaviour:** Again, the four types of risks mentioned above are observed, but in this case they refer to the child's own behaviour when using the Internet, which may put him/her in a vulnerable position by engaging in hateful (cyberbullying, etc.), harmful (*sexting*, etc.), illegal behaviour or participating in the distribution of disinformation.
3. **Contact:** Risks occur in similar categories, but in this case children are contacted by someone who interacts with them through the Internet and makes them

[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

the subject of hate, harmful, illegal or otherwise problematic messages. Clear examples are sextortion, *grooming,* or situations where children provide sufficient data to move from contact in the real environment to contact in the physical environment, with risk to their right to integrity. The difference with conduct risks is that in this case the child is the object or direct victim rather than the actor or active party.

4. **Consumption (contract or consent):** These occur when the child is a customer or consumer, mainly because he or she receives advertising for products that are not appropriate (such as tobacco, alcohol or dating services), because he or she receives advertising that he or she cannot identify as such (e.g. by *product placement* or through an *influencer*), because his or her credulity, inexperience or lack of maturity is exploited to consent to agreements or contracts that are not beneficial to him or her (e.g. by using misleading patterns) or because, directly, it is not up to the child to make decisions about consumption, contract or consent.[5].
5. **Cross-section:** This category includes quite heterogeneous risks that cannot be classified in the previous categories, mainly:
    a. **Privacy** risks**:** such as self-induced overexposure, *sharenting*, processing associated with educational technologies and platforms, etc.
    b. Risks associated with **new technologies:** Such as those associated with the use of artificial intelligence (e.g. tools that produce fake nude photographs offered in video game chats), the Internet of Things (e.g. children's smart watches that allow geolocation), neurodata processing (e.g. to play video games or monitor attention in class) or biometric authentication (e.g. to pay in school canteens or to gain access to a sporting event).
    c. Risks associated with **mental and physical health:** Such as those associated with addictive patterns employed by some services and applications or excessive screen time.

Having understood the main risks to children on the Internet, the following assertions can be made and will be substantiated throughout this paper:

- Age verification solutions, with the right model, can go **a long way to** avoid or mitigate many of these risks **by design and by default**.
- The selection of the appropriate model for age verification, as well as its design and implementation, should be based on a Child Rights Impact Assessment (CRIA).[6]). The management of risks to children on the Internet should not be done blindly or in a rigid or standard way, but after a **systematic and specific assessment of the five categories of risks** already mentioned in the case of a particular application or service, both in terms of its **functionality** and its **target audience**, **context of use**, etc.
- Age verification can use, to manage all these risks, the **enabling approach** that verifies that the user is above the age threshold

[5] Article 7 of the GDPR and the LOPDGDD.
[6] "CHILD RIGHTS IMPACT ASSESSMENTS IN RELATION TO THE DIGITAL ENVIRONMENT: DEVELOPING GLOBAL GUIDANCE", UNESCO, April 2024. https://www.unicef.org/reports/CRIA-responsibletech

required to make configuration changes, allow access to third party communication, install adult applications, etc.

- This allows risks to be managed **proactively**, and gives relatives and guardians back the ability to exercise their duty of care and other obligations.
- The age verification **does not need to verify a specific age or date of birth**, only that the threshold is exceeded. This threshold may be different depending on the type of activity or item you wish to access on the Internet.
- Age verification is useless if **the whole ecosystem** (applications, tools, interfaces, etc.) is not adapted for **child protection by default** and to check that users making certain requests are of the required age to do so in a way that ensures anonymity, non-traceability and that children are not detected.

The remainder of this technical note analyses the four most widespread use cases as described in Table 1, and concludes with a discussion of the principles that should apply in relation to privacy and data protection to ensure that they guarantee not only the best interests of the child, but also the rights and freedoms of all citizens and that they do not create new systemic risks.

Use case analysed	**Risks it includes that can be avoided or mitigated by the age verification**
Protection against inappropriate content	Content
Safe environments for children	Content+Conduct+Contact+Crosscutting
Consent on online to the processing of personal data	Consumption (contract or consent)
4.Age appropriate design	Behaviour+Consumption (contract or consent)+ Cross-section

Table 1. Use cases analysed in this technical note

As will be discussed in the following sections of this note, age verification is an essential tool to avoid or mitigate many of these risks, but it is by no means the only tool; it must be integrated and complemented by other tools, solutions and processes (Figure 1) in a child protection system.

Figure 1. Relationship of age verification to other solutions in the different use cases

IV. MODELS FOR AGE VERIFICATION

In order for age verification to be carried out correctly, one of the fundamental decisions that must be made is its **timing**. Age verification can be performed **at different moments** of a user's interaction with services and applications, and can be performed by different actors. The actors performing age verification can do so with their own solutions or by relying on solutions offered by trusted third parties, the different possible architectures and methods to do so are not discussed in this document.

There is a design principle that must be complied with in any case: age verification must be carried out in the context of access to a service or application **before any further processing of personal data**. In other words, personal data should not be collected from a user and then denied access because the user does not meet the age requirements.

Otherwise, two different models can be distinguished.

A. SERVICES AND APPLICATIONS FOR ADULTS

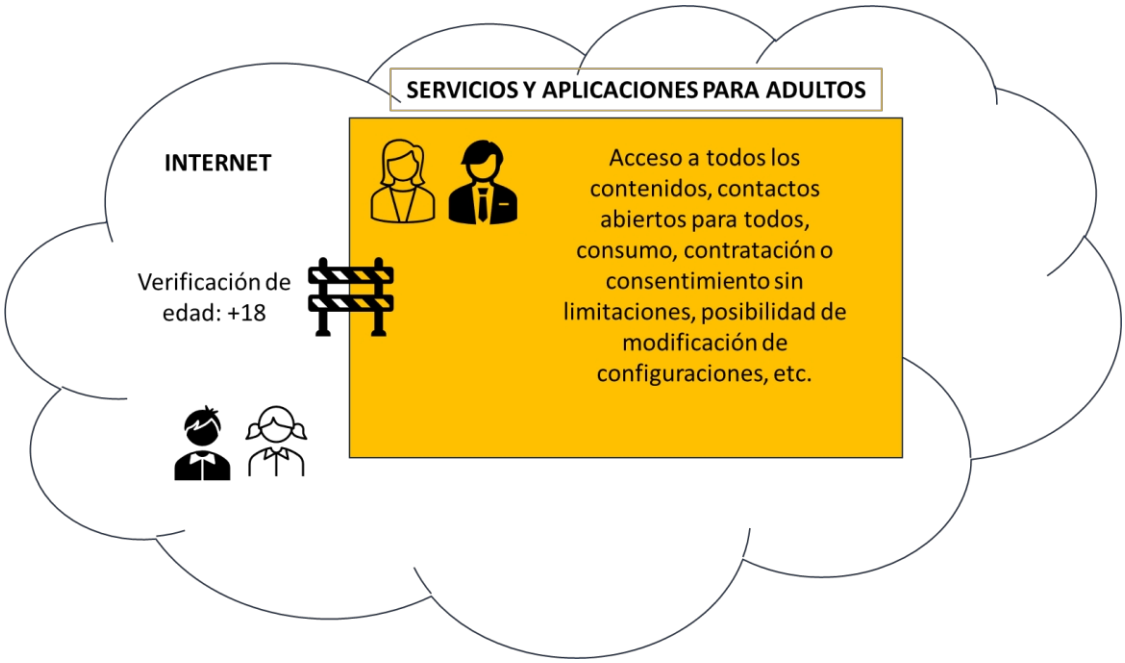

Figure 2. Age verification in adult services and applications

All users are adults, in no case children, who should not be allowed access given its nature and the risks it implies for them.

Who should apply age verification? In the case of an *app*, the relevant *store*, which should verify that the user wishing to download and install the app is above the required age threshold (usually +18). As there are other means of downloading and installing apps, it could also be the provider of the service accessed through the *app* that performs the appropriate checks, for example, the

first time access is made. In the case of a service that can be accessed through a web browser, it is the service provider who should check whether the user is above the required age threshold before creating an account or performing a one-off login. The browser should provide all the necessary support to perform this check properly.

When is age verification carried out? The age verification is, in this model, the entry enabler for the use of the service or the app: in order to start using it, you must prove that you are over the required age. This process should be done at least once, in the *store* or at the provider, in order to be able to download the *app* or create the account.

Should refreshing be carried out at some point? The answer to this question depends on the right balance between different factors: the risk of inference of users' status as minors, the risk that access to inappropriate content poses to children, the risk of manipulation of age verification procedures or usability.

As mentioned above, age verification should always be performed at least once, either to download the *app* or to open the account. It could then be repeated when certain events occur, e.g. device events such as reboots or SIM changes, changes in functionalities or terms of service that may affect age requirements, modifications to user account information such as email, for example (to avoid account handover between users), etc. If the service allows guest access, without the need to create an account, age verification should be performed for each session.

Example of good practice 1

A dating and matchmaking mobile app is suitable for adults only, you must be 18 years or older to install it.

The official *app stores* are responsible for performing age verification before allowing the user to download and install the *app*.

They re-verify with each *app* update.

Example of good practice 2

A pornographic content website is for adults only, you must be 18 or older to create an account and access the content it offers.

Age verification is carried out by the site provider before the user is allowed to create an account.

Please re-verify each time you update the information associated with this user account: username or email address.

Example of malpractice 1

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

The site provider allows all users to create an account, and therefore processes the personal data associated with this creation for all users, without performing any age verification. It does not perform age verification until the moment the user attempts to place a bet.

The personal data of users under the age of 18 is handled completely unnecessarily at the time of account creation, as they are then not allowed to access the service for which the account was created. The flaw lies in the poor design decision as to when age verification should be performed.

Example of malpractice 2

A website with generalist content is for all audiences. It does not offer any other type of content or service that could be classified as "adult" and does not request consent for the processing of personal data.

However, the provider decides to carry out age verification of all its users in order to collect new data (at least age) and to be able to personalise content, advertising, etc. according to the age range to which they belong. Once again, this is a processing of personal data that is not necessary, nor is it proportional. The error lies in the poor design decision to carry out age verification on a site for all audiences that does not involve significant risks specific to children and adolescents.

B. SERVICES AND APPLICATIONS FOR ALL OR MIXED AUDIENCES

In this case, users can be both children and adults. Some content, functionalities or settings are considered suitable for all users while others are considered inappropriate for children because of the risks they may pose and should be protected by age verification.

In this case there are two design alternatives.

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

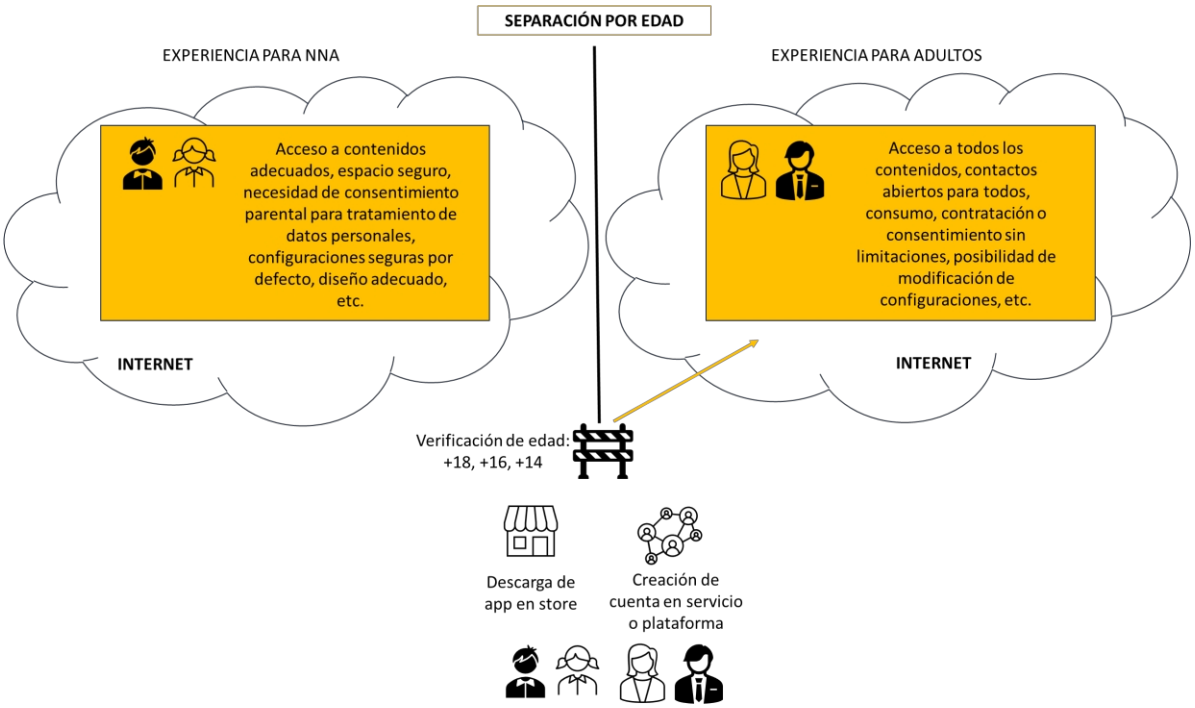

Figure 3. Age verification in services and applications for all publics with age separation

The provider offers two different experiences on its service or application. One version involves default protection for all users so that it only allows access to content, functionalities, settings and elements that are safe or for all audiences, without age restrictions. The other does not involve such protection by default and is used by the user despite the risks it may entail. To do so, he or she must pass an age threshold and prove it.

Who should apply age verification? In the case of an *app*, the relevant *store* should verify that the user who wishes to download and install the default unprotected version of the *app* is above the required age threshold (usually +18). If the *store* is not equipped to perform this type of age verification, the *app* provider could offer a single version for all users to download, the one that offers default protection. Once downloaded, it incorporates a configuration option that requires age verification with the *app* provider, which disables all protections globally. This makes the *app* the version that does not offer default protection after a single age verification process.

If it is a service that can be accessed through a web browser, the service provider should check before creating an unprotected account by default that the user is above the required age threshold, with support provided by the browser.

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

When is age verification performed? As was the case in model 1, age verification is the entry enabler for the use of the service or application, in this case

in its unprotected version by default. This process is usually carried out at least once in the store or at the provider.

Does refreshing have to be done at any point? Same as Model 1.

Example of good practice 3

A social network decides to offer two different versions of its application. The first involves default protection for all users, so it can be used by children and adolescents without posing a risk to them: it does not allow access to content with age requirements, limits contact options with other users (for example, through whitelisting), does not process personal data, has all the secure options configured by default, etc. The other version of the application does not incorporate these protections by default, so it implies a risk that can only be assumed by adults.

The version with default protection can be installed by all users without any age verification. The official *app stores* take care of the age verification before allowing the user to download and install the version without default protection.

They perform the re-verification at each update of the application to a new version.

Example of good practice 4

A live video streaming service decides to offer accounts with default protection and adult-only accounts. Accounts with default protection do not allow access to other age-restricted users' streams, limit contact options with other users (e.g. by whitelisting contacts or interlocutors), do not process personal data, do not allow monetisation of shared content, have all secure options configured by default, etc. All these protections are not offered by default on adult-only accounts.

The creation of accounts with default protection does not require any age verification. The service provider is responsible for performing age verification before allowing the user to create an adult-only account.

Re-check once a month, on a regular basis.

Example of malpractice 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 contact options with other users (e.g. by whitelisting contacts or interlocutors), do not perform any processing, and do not allow access to content inappropriate for children.

They do not allow monetisation of shared content, they have all the secure options configured by default, and so on. All these protections are not offered by default on adult accounts.

The creation of adult accounts does not require any age verification, but the creation of children's accounts does. The social network provider is responsible for age verification before allowing the user to create a child account.

This implies a risk of detection and tracing of children (by a malicious provider, rogue employees, third parties accessing data in an unauthorised manner following a data breach, etc.) and makes the processing not proportionate.

The mistake is in forcing children to verify their age; the default account should always be the one that is safe by default for all users. Age verification should be aimed at verifying that the user willing to take a given risk is old enough to do so, it is an enabling process.

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

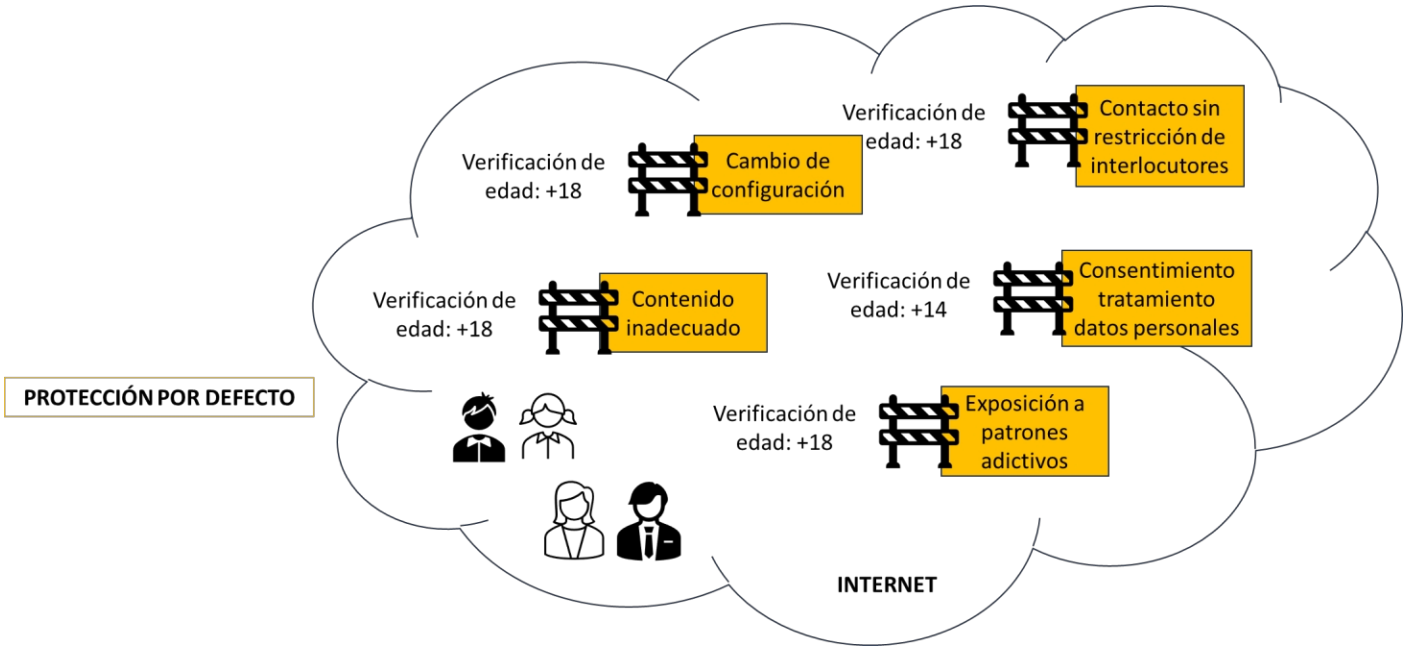

Figure 4. Age verification in services and applications for all audiences with default protection

Sometimes the user's interaction with the service is one-off, anonymous, does not involve any downloading or creating an account, etc. In this case, version 1 of this age verification model is not possible and user experiences cannot be separated by age. Specific age checks must then be performed at specific points in time of such interaction.

Who should apply age verification? The single version of the service or application offered should guarantee protection by default for all users. When a user decides that he or she wants to have access to age-restricted content, functionality or settings because of the risks involved, the provider should check, specifically for that request, that the user exceeds the required age threshold. And it should do so for each request for content, functionality or settings that, because of the risk involved, requires an age threshold to be exceeded.

When does age verification take place? In this case, age verification is likely to be performed more frequently, every time the user wants to access adult content, functionality or settings. And the verification is always done by the service or app provider, as the same version of the *app* (the only one available, with default protection for everyone) is always downloaded from the *store*, regardless of the user's age.

Should a refresh be performed at some point? In principle, an age check should be performed every time a user requests age-restricted content, functionality or settings. If this is to be avoided, "reusable" verifications could be implemented, somehow associating the age verification to the device in the case of *apps* or integrating it with the user's session management in the case of services. In this way, if the user has verified that they are over 18 to access adult content, they can be prevented from having to re-verify to view other adult content immediately afterwards, on the same device or during the same session. But these are very provider-specific design decisions.

Example of good practice 5

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

The *app* incorporates secure default settings (no display of user information, no location sharing, no processing of personal data, limited accessibility to the contact list and no display of messages from other users that have not been explicitly pre-approved, etc.). If a user wants to change any of these settings, he or she has to prove, each time, through an age verification process performed by the *app* provider, that he or she is old enough to do so. For example, they will have to do so in order to be able to receive messages from any user or to start location sharing.

Example of good practice 6

An e-commerce platform does not, in principle, distinguish between users on the basis of their age. All users can browse your website and make purchases without an account, as guests.

But it carries out an age verification process before displaying information on products that are not suitable for children, such as tobacco or alcohol.

If a user proves to be old enough to access the information in this type of product, this information is associated with their session *cookie*, so that no further age verification is required for the duration of the session. Each platform may configure the duration of sessions according to its specific needs.

Example of malpractice 4

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

Safe default settings (no display of user information, no location sharing, no processing of personal data, limiting contacts and not displaying messages from other users that have not been explicitly pre-approved, limiting access to video games with inappropriate content, etc.) can be blocked for a particular account if it is verified that it is for a child. This can be done by the children themselves or by their parents or guardians, in the exercise of their duty of care.

This implies a risk of detection and tracing for children and makes the processing of personal data involved in age verification not proportionate. The mistake is in forcing children to verify their age in order to be protected, when the safe option should always be the default option: always verify that the user is above the age threshold required to perform an activity that poses a risk to children (age verification is an enabler), not the other way around.

V. USE CASE 1: PROTECTION AGAINST INAPPROPRIATE CONTENT

A. PRELIMINARY FRAMEWORK

Uncontrolled access to inappropriate content by children 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, as **all content must be freely accessible to those who can demonstrate that they are above the** established **age threshold**, respecting their fundamental rights and freedoms.

The Spanish Data Protection Agency published in December 2023 different materials in relation to its project on this use case. Specifically, an Infographic with the threats and risks to 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 used to protect minors from inappropriate content. Other European data protection supervisory 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 providing a **harmonised solution** in the member states with different initiatives , , .[11][12][13]

B. LEGAL BASIS

In the following European and national regulations, the need to protect children from unsuitable content is included, with some of the most harmful content being that which depicts gratuitous violence or pornography.

GDPR **recital 38**	Children deserve specific protection of their personal data, as they may be less aware of the risks, consequences, safeguards and rights concerning the processing of personal data. Such specific protection should apply in particular to the use of children's personal data for marketing, personality or user profiling purposes, and to the collection of personal data relating to children when using services offered directly to a child.

[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-systèmes-de-verification-de-lage-mis-en-place-acces-contenus-pornographiques- en-ligne
10https://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

GDPR **recital 75**	Risks to the rights and freedoms of natural persons, of varying severity and likelihood, may result from the processing of data which could lead to physical, material or immaterial damage, in particular in cases where the processing may give rise to problems of discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to professional secrecy, unauthorised reversal of pseudonymisation or any other significant economic or social damage;....in cases where personal data of vulnerable individuals, in particular children, are processed; or in cases where the processing involves a large amount of personal data and concerns a large number of data subjects.
Law 13/2022 of 7 July on General Audiovisual Communication **Article 88**	Platform video-sharing service providers shall take measures to protect: a) Minors from programmes, user-generated videos and audiovisual commercial communications that may harm their physical, mental or moral development.
Law 13/2022 of 7 July on General Audiovisual Communication **Article 89**	1. In order to protect minors and the general public from the audiovisual content referred to in the previous article, video-sharing platform service providers shall take the following measures: a) Include and implement in the terms of service of video-sharing platforms the obligations set out in Article 88 on certain audiovisual content. b) Establish and operate transparent and user-friendly mechanisms to enable users to notify or draw the attention of the relevant provider to content which infringes the obligations set out in Article 88. c) Establish and operate systems through which service providers explain to users the action taken on the notifications or indications referred to in the previous point. d) Establish and implement user-friendly systems that allow service users to rate content that may violate the obligations set out in Article 88. e) Establish and operate age verification systems for users with respect to content that may harm the physical, mental or moral development of minors which, in any case, prevent minors from accessing the most harmful audiovisual content, such as gratuitous violence or pornography. f) Providing end-user-controlled parental control systems with respect to content that may harm the physical, mental or moral development of minors. g) Establish and implement transparent, effective and user-friendly procedures for handling and resolving customer complaints.

	users to service providers in relation to the implementation of the measures referred to in the previous points. h) Provide effective media literacy measures and tools and make users aware of the existence of such measures and tools. i) Facilitate that users, in the event of a complaint submitted by them and not satisfactorily resolved, may submit the conflict to an alternative consumer dispute resolution procedure, in accordance with the provisions of Law 7/2017, of 2 November, which transposes into Spanish law Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution in consumer matters. All of this without prejudice to users being able to resort to the corresponding judicial channels.

C. A FIRST APPROACH

The approach to resolve this use case while protecting the best interests of the child and the rights and freedoms of all users is based on **verifying, whenever access to age-restricted content is made, that the user is over the required age for such access**. When a user cannot prove that he or she is over the required age, the content should be filtered or access to it blocked by 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 the user is of the appropriate age to access any content that may be offered. In other words, this is model A in section IV of this document.

In the case of **services or applications for all publics or audiences** because they offer hybrid or mixed content (some with age restrictions, others without), two scenarios are possible, those explained in models B.1 and B.2 of the same section IV.

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

D. MISUNDERSTANDING EQUIVOCAL

It is common to come across providers who handle age verification as if their ultimate goal is to know the specific age of all users or to

knowledge of which specific users are children. But this is not the case; in this use case **the objective is to protect minors** from inappropriate content. And this objective can be met **without knowing the exact age of users and without subjecting children to verification processes**. With the **enabling approach** of age verification, it is adults who prove that they are "above the required age threshold" to access services, adult versions of *apps* or specific content. Children are thus **protected by default**, without the need to install additional apps or tools, without the need for the child to understand information provided by the provider, and without the need to undergo further data processing. And, in short, **proactively and without the need to take new risks**. To this end, it is essential, not only an age verification process as outlined above, but also that the services and applications themselves implement such protection by default.

It is also common to make the mistake of thinking that any proposed solution for protecting children will be **circumvented or circumvented** and that, for this reason, no protection system should be deployed at all. For example, it is common to hear the argument that it is not worth the effort because children will learn to use VPNs (*Virtual Private Networks*) to access inappropriate content or will end up using an adult's proof of age or credentials, or even forged ones.

First of all, this is a mistake because today's technology makes it possible to design and develop solutions that make it very difficult to circumvent them (although not impossible, as is the case with other types of protection in other application domains).[14] (though not impossible, as is the case with other types of protections in other application domains). Secondly, because the same argument would apply to a multitude of protections for children in other contexts, and yet society understands that **efforts** to protect the majority of children in most cases **implement protection that reaches a high percentage of children and is mandatory**.

[14] For example, if content filtering is done locally by browsers or content access applications installed on the device itself, circumventing protection mechanisms is much more difficult, especially when the age of the children is low.

VI. USE CASE 2: SAFE ENVIRONMENTS FOR CHILDREN

A. PRELIMINARY FRAMEWORK

Different actors in the Internet ecosystem are working to create safe environments for children. **There is no universal, concrete and widely accepted definition** of what a safe online environment or space for children entails, what requirements it should meet or its desirable properties. Unfortunately, this leads to significant misunderstandings that can be exploited by different actors in a self-interested way.

There is currently a fairly widespread approach that is often 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 **exposure to a risk** by a minor, for example, the 5Cs mentioned in the Introduction section of this document, **corrective action** will be taken. All this under **the discretion, supervision and monitoring** of all the actions of the subjects by **Internet actors** whose legitimate interests, given their current business model, may directly collide with the protection of the fundamental rights of all citizens. Moreover, through the use of tools designed to **prevent** families, educators, regulators or authorities **from effectively exercising their various obligations**.

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

The marketing of a service or application thus labelled as a "safe environment" can, in the worst case, allow **malicious actors** to attract, detect or locate children. In other words, such environments can produce a "fishing in a fishbowl" effect. Detection and tracking does not only imply knowing that a given account belongs to a child, but also being able to associate a real-world identity, a physical (geolocation) or digital address, and to have access to him or her to personalise messages, offers etc. Even with the best intentions of the service or application provider, there is always the possibility that a member of the entity may **use** it **illegitimately** or that there may be a **personal data breach** that exposes the child to third parties.

However, the creation of a safe environment should **seek, by design, to mitigate specific threats** to the fundamental rights of children and all Internet users. In order to create a safe space, **it is not enough to accumulate generic protections**, but these must be appropriate to the specific threats identified. Measures or tools to create secure environments must solve specific problems and **not generate new** and even more serious **vulnerabilities**. This requires a holistic view of the measures adopted, which *a priori* protect children, and how they interact with each other.

Secure environments must be secure by design. To this end, **it is not enough to include an additional security layer** on top of the existing infrastructure, but all actors must evolve to incorporate the properties that make environments secure from the design stage. As mentioned in the previous use case, for example, application *stores*, *apps* themselves or browsers. The Internet ecosystem **cannot be treated as a set of independent islands**. To this end, it is

This requires not only **cooperation** between actors in designing their solutions, but also **effective communication** between them when new threats to child safety are identified through an **appropriate governance framework.**

Measures to protect minors must enable those who have a duty of care to exercise their obligations. **The different obligations associated with the creation of** safe environments for minors on the Internet **cannot be delegated and should not be based on acts of faith**, especially in the case of Internet players whose interests lie in monetising users and building loyalty, if not addiction, to their services and applications. Moreover, they must be able to exercise them **by default**, i.e. the lack of knowledge on the part of those who have a duty of care to children about how certain measures or tools work should not be a major obstacle to the protection of children.

The protection of fundamental rights does not only apply to minors, but also **implies the protection of the rights of all Internet users**, in particular the right to act physically and virtually, to non-discrimination, to freedom of education, information, thought, beliefs, privacy and intimacy, etc., but, above all, the protection of physical integrity must be taken into account. It should be remembered that **children and adolescents are not the only group in a situation of vulnerability** due to certain practices of providers of digital services and applications.

B. LEGAL BASIS

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

DSA **recital 71**	... An online platform may be considered to be accessible to minors where its general terms and conditions allow minors to use the service, where its service is targeted at or predominantly used by minors, or where the provider is aware that some of the recipients of its service are minors, for example because it already processes for other purposes personal data of the recipients of its service which reveal their age. Providers of online platforms used by children should take appropriate and proportionate measures to protect children, for example by designing their online interfaces or parts thereof with the highest level of privacy, security and child protection by default, where appropriate, or by adopting rules for the protection of children, or by participating in codes of conduct for the protection of children. ... Online platform providers should not present advertisements based on profiling using data

	personal data of the recipient of the service where they are aware with reasonable assurance that the recipient of the service is a minor. In accordance with Regulation (EU) 2016/679, in particular the principle of data minimisation provided for in Article 5(1)(c) thereof, this prohibition should not lead the online platform provider to hold, obtain or process more personal data than it already holds in order to assess whether the recipient of the service is a minor. Therefore, this obligation should not provide an incentive for online platform providers to capture the age of the recipient of the service prior to its use. This should be without prejudice to Union law on the protection of personal data.
DSA **Article 35**	Risk reduction 1. Very large online platform providers and very large online search engine providers shall implement reasonable, proportionate and effective risk mitigation measures tailored to the specific systemic risks identified in accordance with Article 34, taking into account in particular the impact of such measures on fundamental rights. Such measures may include, where appropriate: a) adapting the design, features or functioning of their services, including their online interfaces; b) the adaptation of its general conditions and its implementation; c) the adaptation of content moderation processes, including the speed and quality of the handling of notifications related to specific types of illegal content and, where appropriate, the swift removal of, or blocking of access to, reported content, in particular in the case of illegal hate speech or cyber-violence, as well as the adaptation of relevant decision-making processes and specific resources for content moderation; d) testing and adaptation of their algorithmic systems, including their recommender systems; e) adapting their advertising systems and adopting specific measures aimed at limiting or adjusting the display of advertisements in association with the service they provide; f) strengthening internal processes, resources, testing, documentation or monitoring of any of its activities, in particular with regard to the detection of systemic risks; g) the initiation or adjustment of cooperation with reliable alerters in accordance with Article 22 and the enforcement of decisions of out-of-court dispute settlement bodies under Article 21; h) the implementation or adjustment of cooperation with other online platform providers or online search engines through the codes of conduct and crisis protocols referred to in Articles 45 and 48 respectively; i) the adoption of awareness-raising measures and the adaptation of their interface online in order to provide more information to the recipients of the service;

	j) the adoption of specific measures to protect the rights of minors, including age verification and parental control tools, tools to help minors report abuse or obtain help, as appropriate; k) ensure that an item of information, whether image, audio or video generated or manipulated that bears a strong resemblance to persons, objects, places or other existing entities or events and that may mislead a person into believing it to be authentic or truthful, is distinguished by prominent indications when presented in its online interfaces and, in addition, provide user-friendly functionality that enables recipients of the service to point out this information.

C. A FIRST APPROACH

Creating safe environments for children without requiring age verification from children themselves is a **complex challenge**, but the **enabling, proactive and default approach** mentioned above can go a long way towards achieving this. The aim is to **balance accessibility and the protection of fundamental rights and freedoms** (including the best interests of the child and privacy) to ensure that the internet is a space of opportunity for all ages.

In this use case, **children and young people** should be **protected from** hateful, harmful or illegal **content**, but also from **tools or functionalities** that place them in a vulnerable position by engaging in hateful, harmful or illegal behaviour, as well as **from interactions** with other users that make them the target of hateful, harmful, illegal or otherwise problematic messages. They must also be protected from cross-cutting risks involving **overexposure**, certain processing of personal data associated 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), **it is not necessary to** design such child-safe environments, as children are not users and do not need to be protected. They are, by default, because of the age verification required to access these services and applications, which ensures that if access has been gained, they are over 18 years of age.

In the case of services or applications **for all audiences**, there are two ways of providing safe environments for children, the B.1 and B.2 models mentioned above. Model B.1 is followed, for example, by many *streaming* platforms, which allow the creation of accounts with default protection, which allows them to be turned into safe spaces. If a service or application predicts that it may have users of different ages, it can offer **different experiences** according to age, building in protection by design for users who do not verify age. This can be achieved with adult-only accounts, different *apps* for adults in phone *stores*, etc. Age verification should always be done by adults, to prove that they are adults when they want to open an adult account (they verify themselves with the service provider) or install the adult version of the *app* (they verify themselves in the store where they download the *app*). In this way, children and adolescents are protected by default, as they will only be able to access accounts with default protection.

In all other cases, model B.2 applies and all users are treated in the same way, with no differentiated experiences. The safe space must be safe for

default and by design for all potential users, who may be of different ages. **Age-restricted content, functionalities and specific features should only be accessible when the user is "above the required age threshold"** because an age verification process checks that the user's age is above the required age threshold in each case. A couple of examples of good practice (5 and 6) have already been provided in section IV of this note. The functionalities and settings available by default should always be the safe ones, and cannot be changed without an age verification process.

In the two scenarios above, where a safe environment for children and adolescents must be created, age verification could be complemented by tools and processes such as:

- **Interlocutor restriction:** These are specific methods and tools that limit children's ability to interact or communicate with other users, so that they are limited to those on whitelists or allowed contacts.
- **Parental involvement and parental control:** In this case through other tools that allow parents to monitor and control their children's account activity without revealing the child's personal data, set up safe searches or establish content or language filters.
- **Educating children about online risks and responsible use of the Internet**: This includes recognising suspicious behaviour and knowing how to report it on specific services and applications.

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

D. MISUNDERSTANDINGS

Many current proposals are based on the aforementioned restriction of interlocutors and parental controls, as well as other tools that are often included:

- **Community moderation: Trusted** adult moderators (verified through extensive 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 inappropriate for children.
- **Peer-to-peer reporting methods:** Tools that allow children to report suspicious behaviour that adult moderators can review.
- **Behavioural analysis:** Machine learning or artificial intelligence-based analysis tools that monitor play patterns, language use or interaction styles to identify and flag behaviour (not users) that is inconsistent with that of a typical child.

But these tools, **by themselves, are insufficient** to establish a safe environment, as they are based on reactive approaches (the child has already been exposed to the risk) and that

do not protect by default. Moreover, it should be analysed on a case-by-case basis whether they comply with **data protection regulations**, because some of these proposals are based on massive processing of personal data, user profiling. Sometimes in automated decisions that can generate serious legal effects, and are also prone to bias. In short, they may violate the rights and freedoms of all users.

In this use case, moreover, there is a widespread misconception that **a safe environment is safe simply because it only allows access to users who are children**. In this case, the age threshold is interpreted in reverse, as it is only "exceeded" when users are below the age threshold. The risks of basing protection on knowing which specific users are children (e.g. child or adolescent accounts) have been explained earlier in this note.

But it is also a **mistake** to assume that an environment is safe because only children are allowed access to it:

- As in the physical world, **a site is not safe just because only children are allowed access**. On the contrary, because it is very likely that they do not have sufficient maturity or experience to be able to deal with the risk situations that arise in such a "playpen" type context or that they themselves generate.
- This scenario **increases the risk of tracing children (the "fishbowl effect" has already been mentioned)** and of making them targets for commercial or malicious purposes (paedophile rings, etc.).
- Access to inappropriate content should be prevented by default for children, but what would prevent a child from sharing it within one of these spaces? Probably one of the moderation or reporting tools listed above, but after the fact, following a **reactive approach that does not prevent exposure to risk**.
- Protections **should not be applied** after the child has already been exposed to risk, in a reactive manner. Protections should be applied in advance, and by default, by default and by design. Only in this way can attempts be made to avoid or minimise the risk and its potential impact.
- The availability of the child for anyone to access him or her over the Internet should be **null and void by default** for anyone outside his or her trusted environment. It is not enough to trust that other users are all of the same age range.
    - A child may be pressured or threatened by an adult, directly or indirectly, to contact other children.
    - Mixing children of very different ages could pose a risk. They should not be treated as a homogenous 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**, making those same third parties a risk.
    - Determining the best interests of a child is an obligation of parents and the other actors already mentioned in this note, and cannot be left to technology companies with legitimate commercial interests.

It should be noted that **no regulatory framework requires the creation of safe spaces where all users are children**. Recommendations to make the internet a safe space for children, and to make it *age-aware*, can always be interpreted in the other direction: only users who are confirmed as

Adults may access certain content, have unrestricted contact with other users, be exposed to certain functionalities or technologies, or modify certain settings.

VII. USE CASE 3: ONLINE CONSENT TO PROCESSING OF PERSONAL DATA

A. PRELIMINARY FRAMEWORK

The current regulatory framework for data protection **allows for the collection and processing of personal data of minors if certain conditions are met**. Consent may be one of the legal bases that legitimise such processing of personal data (Articles 6.1 and 8 of the GDPR, and 7 of the LOPDGDD) or one of the conditions that may allow the lifting of the prohibition on processing special categories of data (Article 9.2 of the GDPR). In this context, consent is any freely given, specific, informed and unambiguous expression of will by which the data subject agrees, either by a statement or a clear affirmative action, to the processing of personal data concerning him or her, and in the case of children under 14 years of age (in other European countries the age limit for consent may be different, but always **between 13 and 16 years of age**), such consent will have to be given by those who hold their parental authority or guardianship. Therefore, the information to obtain such consent should not be tailored to the child, but to the adult decision-maker.

In Spain, minors between 14 and 18 years of age may grant 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 LOPDGDD[15]). To this end, **the controller must make reasonable efforts to verify** that the 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 a controller should use to ascertain whether the user of an online service or application is above this age limit, nor how parental consent should be sought where it is necessary or to demonstrate that it has been sought with due diligence.

B. LEGAL BASIS

The following are some key issues in relation to consent to the processing of personal data in the case of children and adolescents:

GDPR **recital 38**	Children deserve specific protection of their personal data, as they may be less aware of the risks, consequences, safeguards and rights concerning the processing of personal data. Such specific protection should apply in particular to the use of children's personal data for marketing, personality or user profiling purposes, and to the collection of personal data relating to children when using services offered directly to a child. The consent of the holder of parental responsibility or guardianship should not be required in the context of preventive services or services for counselling offered directly to children.

[15] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights): https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

EDPB Guidelines 05/2020 on consent section 7.1	The term "in particular" indicates that the specific protection is not limited to marketing or profiling, but includes the broader scope of "collection of personal data". relating to children".
GDPR **recital 58**	The principle of transparency requires that any information addressed to the public or the data subject should be concise, easily accessible, easy to understand, in clear and plain language and, where appropriate, displayed. This information could be provided in electronic form, for example, when addressed to the public, through a website. This is particularly relevant in situations where the proliferation of actors and the technological complexity of the practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data concerning him or her are being collected, as in the case of online advertising. As children deserve specific protection, any information and communication concerning their processing should be provided in clear and easily understandable language. simple and easy to understand.
EDPB Guidelines 05/2020 on consent section 7.1	As mentioned in section 3.1 on informed consent, the information should be understandable for the intended audience of the controller, with particular regard to children. In order to obtain a child's "informed consent", the controller should explain in language that is clear and simple for children how he or she intends to process the data he or she collects61. If it is the parent who must give consent, a data set may be required to enable adults to make an informed consent decision. informed decision.
GDPR **recital 75**	Risks to the rights and freedoms of natural persons, of varying severity and likelihood, may arise from the processing of data which could lead to physical, material or immaterial harm and damage, in particular in cases where the processing may give rise to problems of discrimination, identity theft or fraud, ... in cases where personal data of vulnerable individuals, in particular children, are processed; or in cases where the processing involves a large amount of personal data and concerns a large number of interested parties.
GDPR **Article 8, Conditions applicable to the consent of the child in relation to information society services**	Where Article 6(1)(a) applies in relation to the direct offering of information society services to children, the processing of a child's personal data shall be considered lawful where the child is at least 16 years old. If the child is under 16 years of age, such processing shall only be lawful if and only to the extent that the consent was given or authorised by the holder of parental responsibility or guardianship over the child. Member States may provide by law for a lower age for such purposes, provided that such lower age is not less than 13 years.

	2. The controller shall make reasonable efforts to verify in such cases that consent was given or authorised by the holder of parental responsibility or guardianship over the child, taking into account available technology. 3. Paragraph 1 shall not affect general provisions of contract law of the Member States, such as rules relating to the validity, formation or effect of contracts in relationship with a child.
Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights **Article 7, Consent of minors**	1. The processing of personal data of a minor may only be based on his or her consent if he or she is over 14 years of age. Exceptions to this rule are cases where the law requires the assistance of the holders of parental authority or guardianship for the conclusion of the legal act or transaction in the context of which the consent is sought for treatment. 2. The processing of data of children under 14 years of age on the basis of consent shall only be lawful if the consent of the data subject is given. of parental authority or guardianship, with the scope determined by the holders of parental authority or guardianship.
EDPB Guidelines 05/2020 on consent **section 7.1**	It is clear from the above that Article 8 will apply only when the following conditions are met: that the processing of is related to company services information offered directly to children, that the processing is based on consent. ... The CJEU has held that information society services information includes the contracts and other services that are concluded or broadcast online. ... if a provider of information society services ceases to provide information society services clear to its potential users that it only offers its services to persons aged 18 or over, and this is not undermined by any other indications (such as the content of the site or the plans of marketing) then such a service shall not be considered to be "offered directly to a child" and Article 8 shall not apply to a child who is application ... In particular, it should be noted that a data controller who cross-border service provision may not always be limited to the compliance with the legislation of the Member State in which you have its principal place of business, but may be obliged to

	to comply with the respective national legislation of each State. member in which it offers the company's service(s) of information ....

	When providing information society services to children on the basis of consent, controllers are expected to take all reasonable steps to verify that the user is above the age of digital consent, and these steps should be proportionate to the nature and risks of the processing activities. ... If users declare that they are above the age of digital consent, the controller may carry out the necessary checks to verify that this declaration is true. ... If the user declares not to be of age to give digital consent, then the controller can accept this declaration without further verification, but must then obtain parental consent and verify that the person giving consent is the holder of parental or guardianship rights. .... Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of the data subject should involve a risk assessment of the proposed processing. In some low-risk situations, it may be appropriate to ask new subscribers to a service to indicate their year of birth or to fill in a form stating that they are (or are not) minors. In case of doubt, the responsible person should review their age verification mechanisms in a particular case and consider whether further checks are required. ... It is up to the controller to determine which measures are appropriate in a specific case. As a general rule, controllers should avoid verification solutions that involve excessive collection of personal data. ... controllers are expected to keep their processing activities and available technology under constant review.
GDPR **Article 12, Transparency of information, communication and modalities of exercise of the**	1. The controller shall take appropriate steps to provide the data subject with any information referred to in Articles 13 and 14, as well as any communication pursuant to Articles 15 to 22 and 34 concerning processing, in a concise, transparent, intelligible and easily accessible form, in clear and plain language, in particular any information specifically addressed to a child. The information shall be provided by

rights of the data subject	in writing or by other means, including, where appropriate, by electronic means. At the request of the data subject, the information may be provided orally, provided that the identity of the data subject is established. interested by other means.
EDPB Guidelines 05/2020 on consent section 7.1	After reaching the age of digital consent, the child shall have the possibility to withdraw the consent himself/herself, in accordance with Article 7(3). child on this possibility
GDPR **Article 40, Codes of conduct**	2. Associations and other bodies representing categories of controllers or processors may draw up codes of conduct or amend or extend such codes in order to specify the application of this Regulation, such as with regard to: ... (g) the information provided to children and the protection of children's rights. The child's parents or guardians must be informed of the child's rights, as well as how to obtain the consent of the holders of parental authority or guardianship over the child;
EDPB Guidelines 05/2020 on consent section 7.1	As regards the authorisation of a parent or guardian, the GDPR makes no practical provision for obtaining parental consent or establishing that someone has the right to take such an action.67 The EDPS therefore recommends a proportionate approach, in line with Articles 8(2) and 5(1)(c) of the GDPR (data minimisation). Therefore, the EDPS recommends adopting a proportionate approach, in line with Articles 8(2) and 5(1)(c) of the GDPR (data minimisation). A proportionate approach may be to focus on obtaining a limited amount of information, for example, the contact details of a parent or guardian. What will be reasonable, in relation to verification that a user is old enough to give his or her own consent or that a person giving consent on behalf of a child is the holder of parental or guardianship rights, may depend on the risks inherent in the processing, as well as on the technology available. In low-risk cases, verification of parental or guardianship by e-mail may be sufficient. Conversely, in high-risk cases, it may be appropriate to request further evidence, so that the controller can verify and retain the information in accordance with Article 7(1) of the GDPR68. Trusted third party verification services may offer solutions that minimise the amount of personal data that the data controller may need to verify and retain in accordance with Article 7(1) of the GDPR68. The person in charge must himself deal with it.

C. A FIRST APPROACH

Taking into account the fundamentals outlined in the previous section, **it should be verified whenever consent is given** online in a service or application for all audiences that

the user providing it is "capable of consenting" or is

"capable of consenting'. In other words, the user must be over the age of 13 to 16 as established by law in his or her country (from the +18 verification of the use cases contemplated so far to +14, for example, in Spain). Where a user cannot verify this capacity, the processing of personal data requiring consent can only be carried out with the consent of those with parental authority or guardianship. If such consent is not given, the consequence could be that **a service is provided in a limited or different way** for these cases, not necessarily that the user cannot use the service.

In this case of services or applications for all audiences, it may happen that they offer different experiences according to age (model B.1 in section IV), such as adult-only accounts, adult *apps* in phone *stores*, etc. **By matching the NNA/adult age restriction with the age of consent** (14 years in the case of Spain), it is possible to prevent the processing of personal data for which the legal basis is consent in versions without age verification (those that incorporate the default protection) or to always request parental consent for such processing by default. Whereas, in the case of the versions for adults, it is known for sure that users are able to give consent when necessary.

If default protection (model B.2) is implemented, all users are treated in the same way, with no differentiated access accounts or *apps*. Therefore, whenever personal data processing is based on consent, it is necessary to **first check whether the user is "capable of consenting"** 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 an 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 the controller, before obtaining consent, must **provide basic information** on at least the identity of the controller, the purposes of the processing, the recipients of the data, and the exercise of rights (Article 13 of the GDPR). And that the request for consent shall be provided in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form and using clear and plain language (Article 7(2)).

This means that **a service does not need to have messages tailored to children under the age of 14, because they do not have to give consent**, it is given by adults who have that duty of care. In turn, if it can have users over the age of 14, the information must also be adapted for them. It must be taken into account that **not all users over the age of 14 are in the same circumstances for** reasons of education, culture, mental capacity, personal circumstances, the urgency of accessing the service, etc. In fact, to try to divide the type of messages between messages for 14-18 and those over 18 is a great simplification.

That is, when a service is intended for all audiences and the user's age and other circumstances are not known exactly, only that he or she is "able to consent", it must be ensured that the rights of all potential users are adequately protected, **by default and by design.**

Although this note focuses on the use case relating to consent to the processing of personal data, a similar approach could be followed for risks associated with other consents or the signing of contracts, acceptance of terms and conditions, etc. It would, however, be necessary to make the appropriate nuances depending on the legal bases.

(in all likelihood it would not apply exclusively to the GDPR), age thresholds, etc.

It should also be recalled that age verification solutions solve part of the problem, but will need to be complemented by other solutions such as **parental consent or consent receipt management** to ensure compliance with all obligations under the GDPR in relation to consent, and in particular the consent of children.

D. MISUNDERSTANDINGS

This use case sometimes shows an **expansive interpretation** of the obligations involved in complying with the GDPR. It is not necessary to know the age of the users of a service in order to comply with the regulation or to know which of these users in particular are children. It is only necessary to know that they **are over the minimum age to grant consent in** those cases in which the service is offered to children and in which it is also necessary to obtain such consent in order to process personal data.

Nor is it necessary in any case to verify the age of the children, as the approach should be the opposite - the user who wishes to give consent must prove that he or she is capable of doing so.

The default protection option is also sometimes criticised because it seems to imply an infantilisation of all users. But **the language involved in the request for consent and in the rest of the communications should be clear and simple for users over the age of 14** (in the case of Spain), who are the ones who are able to consent. At present, this does not imply that messages are childish and may even indirectly benefit all users regardless of their age and circumstances. There is always the option, moreover, of letting the user choose, once their age above 14 has been verified, between different options for messages, explanations, requests, etc. depending on their degree of digital competence, maturity, etc.

VIII. USE CASE 4: AGE APPROPRIATE DESIGN

A. PRELIMINARY FRAMEWORK

The term "age-appropriate design" **does not have a universal, concrete and widely accepted definition either**. In general, when the term 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 categorise children according to their age.

It should be borne in mind that different companies and organisations interact with children in a targeted or specific way, while others interact with children in the course of their general activities, as they do with users of any other age. All of them should take into account use case 3 and what has already been explained in relation to consent to the processing of personal data.

In any case, there is some **obligation to children to provide adequate, or at least not inadequate, services and applications**. But what does this obligation entail, who should assume it and to what extent? Because this use case must be clearly separated from Use Case 2, which refers exclusively to safe environments and therefore relates to protection against content, behavioural, contact or cross-core risks. In this use case 4 **the risks are related to conduct, consumption, consent or contract and other cross-cutting risks**. That is, risks that may also affect the child's best interests or 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", which has been working since summer 2023 on the EU Code of conduct on age-appropriate design (BIK Code).[16] which has been working since summer 2023 on the *EU Code of conduct on age-appropriate design* (BIK Code). This code has not yet been made public, but other **codes of appropriate design for children** have been published, such as the ICO code[17] , the first one published, or the *California Age Appropriate Design Code*[18] (which is awaiting a court decision before it can be implemented).[19]). Different countries are currently working on new drafts of which some details have already been shared.

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

16 https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design
17https://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/

B. LEGAL BASIS

The concept of age-appropriate design is cross-cutting, as the rights of children and adolescents, their well-being and the protection of their best interests appear in many and very heterogeneous regulations. Mentions of age-appropriate design can be found in European standards of:

- Data protection (already discussed in the previous use cases).
- Consumer protection.
- Security and protection of physical, sexual and abuse integrity.
- Digital services, products and markets.
- Education.
- Health.
- Equality.

The fundamental difference with the three use cases already discussed in this paper 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 previous use cases, **services or applications for adults do not have to worry about providing child-friendly design**. It is services or apps for all audiences that may consider doing so, and two scenarios are distinguished.

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

In the case of default protection (model B.2), all users are treated in the same way because their age, and whether they are above a certain age, is not known. Code standards should be applied to all users so that **children are always exposed to a design that is appropriate for them**. This ensures that their needs are respected and their best interests are protected. **Adults verifying their age will be able to modify this design or default settings if they wish to do so**. This approach can be beneficial for less digitally competent users, older people or those with certain disabilities, to name but a few examples.

In relation to the latter, good practice, in general, is **not to link digital maturity or competence with age**. All users (not just children) should have the option of voluntarily accessing different design versions of the interfaces of the services and applications they use according to their needs and preferences. This **adaptive design** need not necessarily be based on age-verification processes, but on giving users options to freely choose the ones they feel are most appropriate, useful or beneficial to them. **Browsers or applications for accessing different services can provide important support for such adaptive design**, so that the user does not need to

The Commission's proposal is based on the fact that it is possible to make its selection on a case-by-case and case-by-case basis, but that its decisions can be recalled or automated based on certain settings or preferences.

D. MISUNDERSTANDING EQUIVOCAL

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

In summary, the first is the one already discussed throughout this note of basing the solution on knowing which specific users are children and adolescents and on the supposed **need to know their specific age. The second is to confuse age or age range with degree of maturity**, which varies between genders and educational and cultural situations, for example. As explained above, with the enabling, proactive and default approach to age verification, it is older people who, in some cases, will have to verify their age in order to access a design that is appropriate or comfortable for them, and not the other way around. And also only when they want this type of adaptation, as it could happen that due to their degree of maturity or other circumstances they prefer the default interface that is considered suitable for children (this only with model B.2, with A and B.1 they will have a different default interface than the one suitable for children).

The third is for an ISP to predetermine what level of maturity a child has based on their age or age range, **rather than the family, or even the child**, being able to choose what design they wish to use based on their personal circumstances. Providers should not dictate how a child uses the Internet based on their own particular criteria.

And the fourth is the lack of concreteness or standardisation of the term "child-friendly design". One answer may be that it is more persuasive or addictive for children, making this type of design **a misleading pattern that should be avoided because of the risks involved.**

IX. IMPLEMENTATION OF THE DECALOGUE PROPOSED BY THE EPPD

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

But, as discussed in the previous sections, age verification solutions can be used in **scenarios other** than this one, so the question arises whether the proposed decalogue of principles can be directly applied to these use cases that are not exclusively related to protection against inappropriate content but to protection against other types of risks.

The answer is yes, as the approach to using age verification as a fundamental tool in the protection of children 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), placing 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. It would simply be necessary to **generalise the language** in which these principles are expressed to make them applicable to all use cases:

- **Principle 1:** Age verification should not make it possible to identify, track or trace minors via the Internet.
- **Principle 2:** Age verification should enable age-eligible persons to prove their status as "over the required age threshold", and not the other way around, to prove their status as "under age" or "not over the required age threshold".
- **Principle 3:** Proof of exceeding the required age threshold should be anonymous to ISPs and third parties.
- **Principle 4:** The obligation to prove the status of a person "above the required age threshold" shall be limited only to processing operations where such proof is necessary.
- **Principle 5:** Age verification should meet the requirements of accuracy, adequacy and data minimisation. For the latter, it should categorise whether the person "exceeds the required age threshold" or equivalent.
- **Principle 6:** Age verification should not make it possible to profile individuals on the basis of their Internet browsing.
- **Principle 7:** Age verification should not make it possible to link an individual's activity between different Internet services.
- **Principle 8:** Any solution to age verification should ensure the exercise of parental authority by parents where the case of use so requires.
- **Principle 9:** Any solution to age verification must guarantee the fundamental rights of all individuals in their access to the Internet.
- **Principle 10:** Any age verification solution should have a defined governance framework.

X. CONCLUSIONS

A safe Internet by default means **guaranteeing children and adolescents (children and adolescents) their rights and freedoms in the digital environment** by minimising the risks associated with harmful content, contact with other people, inducing 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 make the Internet safe by default and can help manage the risks associated with the 5Cs: Content, Contact, Conduct, Consumption (consent or contract) and Cross-Cutting. This is reflected in various **national and European regulations that impose obligations** on Internet actors. However, it should be borne in mind that age verification solutions alone are not enough to protect children on the Internet. Internet services and the tools that allow access to them (such as applications offered in *stores* or browsers) must **properly integrate** age verification with other solutions and tools in order to effectively protect children and the rights of all citizens.

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

There are **misunderstandings, errors, ambiguities and misrepresentations** in relation to child online protection, in particular its requirements, desirable properties or implications. Some of the most dangerous misunderstandings **relate to 'safe environments', 'child-friendly accounts' or 'child-friendly' design**. In many cases it is proposed to know **which specific users are children** in order to configure and monitor their activity. This poses a risk, as the child 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 children is that information for decision-making must be adapted to a language they can understand, for example, in the case of terms of service. However, making decisions to consent to personal data processing, contracting or consenting to contact with other users is an obligation, the duty of care, which is legally incumbent on those with parental or guardianship rights. **It is not necessary to adapt language for children and adolescents to make decisions that, according to their age, do not even correspond to them**.

Another excuse used to target children is the adaptation of digital environments or designs to their age. However, this implies either that minors have to be in Internet environments that offer the same features and functionalities to all users between 5 and 14/16/18 years old, or that greater granularity is required in determining the age of the child. In either case, these users are forced to conform to "average" or provider-defined standards. Again, there is a risk of keeping children in separate 'pen-like' spaces. Moreover, these approaches may seek to **legitimise the processing of children's data,** and thus of all users, and hide purposes of more precise profiling in relation to deceptive and addictive patterns, loyalty, recruitment, consumption or monetisation of personal data. In addition, in many cases they involve the use of new

Internet identity management, either specific to minors or to all users, which collect personal data outside the guarantees of identity developed in national or European regulation, dependent on services (sometimes located outside the EU), with no guarantee of availability. And, what could be more worrying, they turn people's identity, a right, into a service.

Another common misconception is that of a safe Internet by default based solely on **reactive** strategies: letting children's personal data be processed, exposing them to risk and, ideally, reacting when harm is detected. This involves exposing the child to, for example, being contacted by any user; subjecting all users to surveillance and profiling techniques; accumulating evidence of harassment or paedophilia; applying criteria set by the service provider; and finally taking action. This strategy requires harm to the child and, in addition, intrusive and systematic intervention in the privacy of all users, making **the processing of personal data involved unsuitable and unfair.**

This note explains how to achieve a safe internet by default with **a paradigm** shift that rejects all these misconceptions. The approach to managing risks to children should always be **proactive**, focused on prevention and with the intention of avoiding or minimising impacts and harms, not reacting once they have occurred. The approach should be **enabling**, so as to verify that users are above the age threshold required to perform an action or access an item on the internet. This avoids subjecting children and young people to age verification (with the consequent processing of personal data), who are **protected by default**. Therefore, the child does not have to prove that he or she is a minor, nor does he or she have to expose his or her nature in order to have content, contacts, behaviour or contracts "blocked". On the contrary, this paradigm returns to family members and guardians the ability to exercise their duty of care, shifting the burden of proof to users who are able and willing to take risks.

A safe Internet by default can be achieved by applying the **decalogue** of principles proposed by the AEPD for age verification in all the cases of use analysed and in others that may arise in the future 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 in the framework of the four cases of use described is the protection of children and adolescents.

Design decisions for these solutions should always be based on rigorous processes **based on** both technical and scientific **evidence** (e.g. in relation to the physical and mental integrity of children) and **risk management** for children's rights and data protection of children and users in general, and not on intuition, fads or beliefs. Therefore, decisions for the management of these risks to children should be based on a **child rights impact assessment (CRIA)**, and the processing that is implemented for this purpose, in particular age verification processing, given the **high risk** to the rights and freedoms of individuals, on a **personal data protection impact** assessment (PPRIA) to be carried out by the controller of such personal data processing.

In order to overcome this EIPD, the principle of data minimisation, among others, must be complied with and, in the case at hand, age verification does not require, in any of the analysed use cases, verification of a specific age or date of birth, only the exceeding of the necessary age threshold. Furthermore, all reasonable steps must be taken to ensure that the data processed in age verification processes are **accurate** with respect to the purposes for which they are processed, i.e. a level of accuracy must be guaranteed.

of sufficient certainty when verifying that a user is above the required age threshold, as this is what allows the purpose of the processing, to protect the child from the aforementioned risks, to be fulfilled. This ensures the adequacy of the processing of personal data that is carried out to verify age.

In particular, it is not enough to layer cybersecurity over the internet ecosystem. Internet service providers have an **obligation** to evolve to **implement data protection principles by design and by default**.

The internet ecosystem **cannot be treated as a set of independent islands**. Effecting a paradigm shift in the protection of children requires not only **cooperation** between stakeholders in the internet ecosystem in designing solutions, but also **effective communication** between them in identifying new threats through a **governance framework.** This includes Internet providers, manufacturers, intermediaries and other Internet operators, as well as data protection, consumer and market regulation authorities, especially for products and services offered on the Internet. Also governmental and non-governmental organisations whose purpose is the education and protection of minors, both Spanish and European. And of course, those responsible for the processing of personal data who consume or use these products and services offered on the Internet and those who have parental authority or guardianship over children and adolescents.

XI. BIBLIOGRAPHY

Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights. BOE no. 294, of 06/12/2018. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Law 13/2022, of 7 July, General Audiovisual Communication. BOE no. 163, of 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 June 2016 on the application of the principle of subsidiarity in the field of health and safety at work of April 2016 on the protection of individuals with regard to the protection of individuals 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/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

DIRECTIVE (EU) 2018/1808 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2018
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), taking into account the evolving market realities. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32018L1808

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 (the Digital Services Regulation). https://eur- lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065

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-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 Commission. 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