POLICY BRIEF

Mind the Gap

Age Assurance and the Limits of Enforcement under EU Law

Jessica Galissaire

October 13, 2025

Tech analysis and policy ideas for Europe

interface

Table of Contents

Executive summary

Children and young people today grow up in a highly connected digital environment that provides access to educational content, entertainment, and peer communities but also exposes them to significant risks including cyberbullying, grooming, harmful or pornographic content, addictive design features, and the misuse of personal data. These risks are not only well documented in academic literature and civil society reports; they have also become a central concern for policymakers at the European Union (EU) and EU Member State levels.

In early June 2025, French president Emmanuel Macron announced his intention to have social media banned in France for under-15s 'in the coming months' if no progress was made at the EU level on this matter. Since then, the French Delegate Minister for AI and Digital Affairs, Clara Chappaz, has been on a crusade to rally other Member States to the cause. Cyprus, Denmark, Greece, Italy, Slovenia, and Spain soon joined forces in supporting the idea of having EU-wide age check mechanisms. Just over two weeks after President Macron's announcement, 21 ministers from 13 Member States signed an op-ed asking to take decisive action 'now' to protect children online. For them, the existing legal framework 'remains insufficient'.

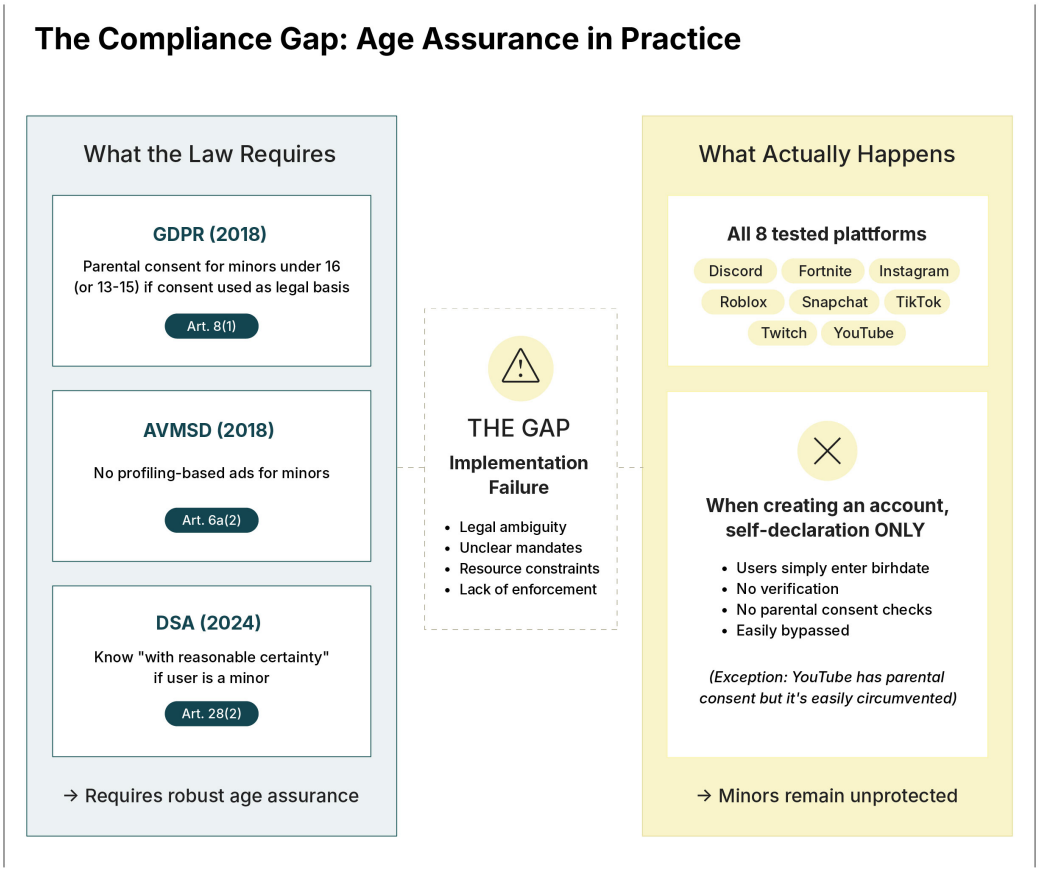
Over the past fifteen years, though, the EU has adopted an increasingly dense set of measures and instruments to protect minors online. The General Data Protection Regulation (GDPR), the Audiovisual Media Services Directive (AVMSD), the Digital Services Act (DSA), and the Artificial Intelligence Act (AI Act) all contain provisions that specifically address children's vulnerabilities. Complementary non-binding instruments—such as the Better Internet for Kids+ (BIK+) Strategy—reinforce the EU's commitment to providing a safe and empowering digital environment for minors. At the Member State level, governments have introduced their own rules and enforcement models, notably France with its *Loi SREN* and Germany with its long-standing *Jugendmedienschutz-Staatsvertrag*.

However, despite these initiatives, minors remain insufficiently protected. The gap between what the existing framework requires and what happens in practice is striking. **This paper's central argument is that the key problem today is not a lack of legislation or awareness but a failure of implementation and enforcement.**

The paper explores this claim through the lens of **age assurance**, understood as the set of technical and procedural mechanisms used to determine the age or age range of a user. Age assurance is a prerequisite for enforcing many legal obligations, from banning targeted advertising to minors (as requested by the DSA and the AVMSD)

to requiring parental consent for data processing (as mandated for certain types of data collection and processing under the GDPR). It is thus frequently presented, in public and political debates, as the cornerstone of online child protection. However, in practice, it is often one of the weakest links in the online child protection chain.

To substantiate this claim, this research goes beyond legal analysis and incorporates empirical testing of the most popular platforms among minors in the EU: Discord, Fortnite, Instagram, Roblox, Snapchat, TikTok, Twitch, and YouTube. The results are unambiguous: all tested services rely on self-declaration mechanisms for age checks when an account is created. None have implemented robust age assurance, and where parental consent tools do exist (notably on YouTube and Fortnite), they can either be easily bypassed or they are applied only after the account has already been created. In practice, minors can thus access these services freely, while platforms remain noncompliant with provisions that legally oblige them to treat minors differently than other users.



This empirical evidence highlights three interrelated issues. First, **the ineffectiveness of self-declaration** as an age assurance method, widely acknowledged as inadequate by regulators and child-rights organisations. Second, the **systematic absence of compliance,** for instance when platforms rely on the 'performance of a

contract' as a legal basis for processing minors' data under the GDPR, without checking whether the user actually has the legal capacity to enter into contracts under national law. Third, the overall **failure of enforcement,** whereby competent authorities either lack the resources, the clarity of mandate, or less optimistically the will to sanction noncompliant practices.

This paper situates these findings within the broader legal and political landscape. At the EU level, debates on age assurance are intensifying. Some Member States, including France, Denmark, and Greece, advocate for EU-wide mandatory age checks or even bans on social media platforms for individuals under a certain age. The European Commission has released detailed guidelines under Article 28 of the DSA, dealing with the protection of minors online, which largely put the emphasis on age assurance. Industry actors, meanwhile, are divided: some (e.g. Meta, Aylo) argue for parental consent or age assurance mechanisms at the operating system level, while others (e.g. Google, Apple) resist such an approach. These conflicting positions reflect different business interests. Overall, unresolved tensions around the pros and cons of age assurance mechanisms show how difficult it can be to reconcile key concepts and rights such as protection, privacy, and proportionality.

Against this backdrop, **this paper makes three key contributions:**

- **It maps the regulatory framework.** It provides a comprehensive overview of the EU instruments that already mandate or imply age assurance, highlighting overlaps, contradictions, and the challenges of multilevel governance.
- **It documents the implementation gap.** Through original empirical tests, it demonstrates that major platforms are failing to meet their obligations in practice, exposing minors to risks that EU law was designed to prevent.
- **It offers actionable recommendations.** The paper proposes measures to strengthen enforcement without adding yet another legislative layer. These include clarifying the mandates of enforcement authorities, improving coordination between EU and national-level bodies, and supporting the development of by-default and by-design tools that safeguard the rights of all users, not just minors, in online environments.

The central message is that, in the short run, more legislation is not the solution. Instead, the EU and Member States should focus on making the existing rules work by ensuring that minors' rights are not just recognised in law but protected in practice. Only by closing the implementation gap can Europe fulfil its ambition of providing children with a digital environment that is truly safe, empowering, and respectful of their rights.

Introduction—Protecting minors online: a growing concern

The extended connectivity that emerged at the beginning of the 21st century brought exciting promises for children and teenagers: facilitated access to information, educational and recreational content, greater connection to peers, ease of communication, and opportunities for creativity and expression. However, with these new opportunities came a series of downsides, including cyberbullying,[1] grooming, exposure to illegal or harmful content,[2] and excessive capture of attention—with sometimes devastating consequences on mental and physical health. In a recent study, Chen *et al.* observed that '[i]n the attention economy, online platforms are incentivized to design products that maximize user engagement, even when such practices conflict with users' best interests'. Through a structured analysis of the design features used by very large online platforms (VLOPs) to capture attention and extend engagement, they found that 'VLOPs use four strategies to extend teens' use: pressuring, enticing, trapping, and lulling them into spending more time online'.

These harmful developments are not only well documented in the academic literature. Protecting children and their rights online has increasingly become a key objective for legislative bodies, governments, regulatory authorities, and civil society organisations around the world. As we will see in the following, the past years have brought numerous legally binding as well as nonbinding initiatives at the European Union (EU) and EU Member State levels. Yet, they have still not provided children with sufficient and effective protection and empowerment, nor have they silenced the ongoing debates around what more can be done. As this paper demonstrates, this is in great part due to an **implementation and enforcement gap between what the existing instruments require and what happens in practice**. To substantiate this claim, this research goes beyond **legal analysis** and incorporates **empirical testing** of the most popular platforms among minors in the EU: Discord, Fortnite, Instagram, Roblox, Snapchat, TikTok, Twitch, and YouTube.

In the last 10 to 15 years, the EU has made the protection of minors online an increasingly hot topic on its policy agenda. In 2012, the European Commission adopted its 'Better Internet for Kids' (BIK) Strategy, whose aim was to address the

1 According to the EU Kids online 2020 survey, about 1 in 10 children becomes a victim of online bullying every month, and an equal number say they never feel safe online.

2 In this paper, 'harmful content' is to be understood as content that can have detrimental effects on body image, self-esteem, and mental health, or content promoting suicide, eating disorders, or extreme violence, for instance.

'particular needs and vulnerabilities' children face on the Internet. Ten years later, to account for the fast-paced evolution in technology, children's digital usage, and legal developments, the Commission released an updated version of the communication: the 'New Better Internet for Kids' (BIK+) Strategy. This revised version proposes actions organised around three pillars: safe digital experiences, digital empowerment, and active participation.[3] The BIK+ Strategy now serves as the blueprint for online child protection and empowerment at the EU level. Numerous instruments give life to it, including legally binding and nonbinding ones.[4] Despite this rich framework, which goes from protecting children's personal data to making sure they do not access online content that may impair their physical, mental, or moral development, the last year has seen a growing number of voices arguing that these measures are insufficient. They are calling for far more extensive action.

Among the possible levers to better protect children online, one has been occupying centre stage: compelling providers of digital services to implement effective age assurance mechanisms to make sure children and teenagers do not access content, products, or services they should not be exposed to. In public and political debates, age assurance, understood as the set of technical and procedural mechanisms used to determine the age or age range of a user, is often presented as a key building block of online child protection. For this reason, it is the central focus of this paper.

Following calls from some Member States, the European Commission has made age assurance one of its top priorities and has released the prototype of an age verification application to be used across the EU. At the European Parliament, some members of the Committee on the Internal Market and Consumer Protection (IMCO) are advocating for a new legislative instrument to tackle age assurance. In June 2025, 21 ministers from 13 Member States deemed the existing framework insufficient and demanded the implementation of mandatory age verification mechanisms across all social networks. In addition, a coalition of Member States including Denmark, France, Greece, and Spain is pushing for a social media ban for individuals under a certain age. Following these developments, President Ursula von der Leyen announced the creation of a panel of experts to advise her on the pros and cons of such a solution.

On the industry side, Meta is calling for parental consent to be imposed to access social media platforms under a certain age. While the Facebook and Instagram parent company argues these checks should take place at the operating system or app-store level—a position that is shared by Aylo, who operates major porn websites Pornhub, RedTube and YouPorn—the likes of Google and Apple unsurprisingly

3 European Commission, 'A European strategy for a better internet for kids – (BIK+)'.

4 Appendix 1 offers a comprehensive overview of these instruments.

disagree, as this would make them the main bearers of the burden. Debates around age assurance at the EU level are lively, bringing together a mix of genuine concerns for children's rights and safety, self-interested proposals, and purely political declarations, as well as concerns related to users' privacy.

When it comes to protecting children and ensuring their rights online, awareness is clearly no longer the issue. These questions have been on the radar of EU policymakers, global institutions, civil society, and—to some extent—the industry for quite some time. There is also no lack of rules or guidance at the EU level—there are plenty of them. And yet, both research and experience repeatedly show that minors are still not adequately protected online. This raises the following questions: How can the implementation and enforcement of the existing rules be improved? Are the current framework and focus flawed and, thus, inefficient? And if so, what would be some more effective measures and approaches?

By focusing specifically on age assurance, this paper aims to answer these questions. In the hope of feeding into the public debate and provide guidance to key stakeholders on the most efficient and speedy way forward, it formulates concrete recommendations for policymakers, as well as NGOs, civil society organisations, and digital service providers.

Age assurance in the EU: the current state of play

When it comes to protecting children online, a lot of the recent media and policy attention has been focused on **age assurance:** the putting in place of technical and procedural mechanisms aimed at checking the age of an internet user, with varying degrees of certainty.

What is age assurance?

'Age verification: A system that relies on hard (physical) identifiers and/or verified sources of identification, which provide a high degree of certainty in determining the age of a user. It can establish the identity of a user but can also be used to establish age only.

Age estimation: A process that establishes a user is *likely* to be of a certain age, fall within an age range, or is over or under a certain age. Age estimation methods include automated analysis of behavioural and environmental data; comparing the way a user interacts with a device or with other users of the same age; metrics derived from motion analysis; or testing the user's capacity or knowledge.

Age assurance: An umbrella term for both age verification and age estimation solutions. The word 'assurance' refers to the varying levels of certainty that different solutions

offer in establishing an age or age range.'

Source: 5Rights Foundation (2021), 'But how do they know it's a child? Age assurance in the digital world', p. 6

Several of the legal provisions exposed in this paper's overview of the rules safeguarding minors online in the EU (see Appendix 1) imply the necessity to offer a different online experience to minors than to adults. Under the AVMSD (article 6(a)(2)) and the DSA (article 28(2)), for instance, the personal data of minors shall not be processed for commercial purposes, such as targeted advertising. Under article 28(1) of the DSA, '[p]roviders of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service'. To some extent, **to comply with these obligations, regulated entities must be able to differentiate minors from adults within their user bases.**[5] To make sure this is done with a satisfactory level of certainty, some EU Member States have introduced laws mandating age assurance and sometimes even technical guidelines on how age checks should be conducted.

Examples of key Member State policies

As shown in a recent report by the Centre on Regulation in Europe (CERRE), France, Germany, Italy, and Ireland have all put in place legally binding rules mandating age assurance to ensure that minors do not access certain content. These measures, however, all have their limitations—hence the recent calls for action at the EU level. **The French and German experiences, detailed hereafter, are particularly informative as to why the Member State level may not be the most accurate and effective one to act.**

Focus: France

In May 2024, France adopted its *loi visant à sécuriser et réguler l'espace numérique* (a law aimed at securing and regulating the digital space), also known as *Loi SREN* or the 'SREN Act'. Article 1 of this law entrusts Arcom, the French Regulatory Authority for Audiovisual and Digital Communication, with the task of establishing a set of standards specifying the minimum technical requirements that age assurance systems used by pornographic websites must comply with. These guidelines were published by Arcom on 11 October 2024 and are enforceable since 11 January 2025.

5 Another option would be for digital service providers to comply with these provisions across the board, irrespective of whether the user is an adult or a minor. This, however, does not seem to be the path they have chosen so far.

If websites hosting pornographic content do not comply with these standards, they risk harsh sanctions, including financial penalties going up to €150,000 or 2% of their global turnover for the last year, whichever is higher—or up to €300,000 or 4%, respectively, in the event of repeated noncompliance. In addition, the French regulator can, after formal notice, order internet service providers to block noncompliant websites for up to two years and order search engines to delist these websites within 48 hours. **However, until recently, these measures were only applicable to websites established in France or outside the EU, as the EU has competence for those established within its territory.** Major websites such as Pornhub, RedTube, and YouPorn (hosted by Aylo Freesites Ltd, based in Cyprus), for instance, were thus out of scope.

To fill this gap, France issued a ministerial order on 26 February 2025, which entered into force three months later. Inspired by article 3(4)(b) of the EU's eCommerce Directive, this decree extends the above-mentioned obligations to a series of 17 websites hosted in other EU Member States. Hammy Media Ltd, who operates xHamster, one of the 17 targeted websites, contested the French ministerial order before the Paris Administrative Court, which validated their claims and suspended the order. The French Minister of Culture and the Minister for AI and Digital Affairs, who authored the order, then referred this decision to the *Conseil d'État* (Council of State), France's highest administrative law court, which overruled the previous decision and reestablished the ministerial order on 15 July 2025.

As mentioned in this decision, on 6 March 2024, the *Conseil d'État* also 'referred a question to the Court of Justice of the European Union for a preliminary ruling regarding the possibility of applying [this order] to companies based in other Member States of the European Union, in an appeal concerning the provisions of the 'SREN Act''. At time of writing, a decision from the CJEU is still pending.[6]

In May 2025, the European Commission opened proceedings against four pornographic websites under the Digital Services Act. In preliminary investigations, it found that these platforms had failed to take '[a]ppropriate and proportionate measures to ensure a high level of privacy, safety and security for minors, in particular with age verification tools to safeguard minors from adult content'. Three of these websites (Pornhub, XNXX, and XVideos) are also covered by the French order under the SREN Act. **These overlaps raise questions as to the efficiency of the existing legal framework and as to the most appropriate level to take action to protect minors from accessing such content.**

6 Advocate General of the Court of Justice of the EU Maciej Szpunar made his legal opinion public on 18 September 2025, but the Court itself has not ruled on the case yet at time of writing.

In addition to the SREN Act, on 7 July 2023, France adopted a law 'establishing digital majority and combating online hate'. It imposes a requirement on social media platforms operating in France to refuse the registration of minors who are under 15 unless consent is given by one of the minor's legal guardians. This means that: 1) such platforms must check the age of their users to know whether they are over 15, and 2) if the person is under 15, they must implement a technical mechanism allowing the collection of parental consent. This provision also applies to already existing accounts, meaning that social media platforms must check the age of all their existing users based in France and, for those who are under 15, obtain the consent of their legal representative. For the age check to be valid, the platform must comply with the above-mentioned technical guidelines published by Arcom. Noncompliant actors face fines of up to 1% of their global turnover for the previous year.

This provision, however, has never been enforced. Although the text was notified to the European Commission in early June 2023 under the Technical Regulation Information System (TRIS), the European executive power found that France did not fully comply with the notification procedure. In a letter sent to the French Minister for European and Foreign Affairs, Thierry Breton, then EU Commissioner for the Internal Market, also criticised this law for undermining the 'direct applicability of the Digital Services Act'. He demanded that France repeal the provisions enacted and restart the procedure from scratch. This was never done, and French President Emmanuel Macron himself recognised in May 2025 that this was a prerogative of the EU. Since then, France, led by its Minister for AI and Digital Affairs, Clara Chappaz, has been pushing this topic at the EU level.

Lessons learned from the French experience

France's push for strict age assurance rules illustrates the growing tension between national initiatives and EU-level competence in regulating online safety for minors.

- France has gone further than most Member States in trying to enforce age-verification on large platforms, even extending obligations to providers based elsewhere in the EU.
- However, this approach exposes legal and political fault lines: its measures collide with the EU's 'country of origin' principle, raise questions at the Court of Justice, and overlap with parallel enforcement under the Digital Services Act.
- Piecemeal national laws risk legal fragmentation and uneven enforcement across the EU, reinforcing the case for coherent EU-level action on age assurance and the protection of minors online.

Focus: Germany

Germany is another particularly interesting case to study when it comes to age assurance. It has one of the longest experiences in enforcing age restrictions to access certain content, especially pornographic content. The *Jugendmedienschutz-Staatsvertrag* (Youth Media Protection Interstate Treaty)[7] abbreviated JMStV, which has been effective since 2003[8] and covers 'telemedia' (i.e. the Internet, television, and radio), makes it illegal to make pornographic content accessible to minors. As mentioned in §4(2), hosting pornographic content is only permissible 'if the provider ensures that [it is] only made accessible to adults (closed user group)'.[9]

Technically, this mandates age assurance, as electronic media hosting pornography must ensure that their content can only be accessed by adults. Not doing so is considered a criminal offence, as is now the case in many other countries. German authorities thus have 22 years of experience in age assurance enforcement. To make it as effective as possible, they have developed quite a unique model, called **'regulated self-regulation'**, which is neither coregulation nor mere self-regulation.

The Commission for the Protection of Minors in the Media (*Kommission für Jugendmedienschutz* or KJM) is the primary authority responsible for the enforcement of the treaty. It may issue fines of up to €500,000 in the event of serious violations or require the age-gating of inappropriate content. In addition, 14 *Landesmedienanstalten* (State Media Authorities)[10] cooperate with the KJM in overseeing enforcement.

To complement this oversight, organisations such as the Association for Voluntary Self-Regulation of Digital Media Service Providers (*Freiwillige Selbstkontrolle Multimedia-Diensteanbieter* or FSM) have a legally binding role under the JMStV. Telemedia companies are encouraged to join the FSM and develop their own rules for how to comply with their child protection obligations under the interstate treaty. In the area of age assurance, this 'regulated self-regulation' has led to the certification of no less than 120 age-assurance mechanisms by either the KJM or the FSM. The regulated entities thus have a pool of technical solutions available to verify the age of their users that have been deemed legally compliant by the authorities. In addition, for those organisations who have joined the FSM as members, it is not the KJM or the State Media Authorities who are in charge of ensuring they respect their child safety obligations under the JMStV but the FSM itself. In order to be given this role,

7 The full name of the treaty is *Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien*, which translates to the Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and Telemedia.

8 And was last amended in 2022.

9 Own translation.

10 One per State (or *Land*), with the exception of Berlin and Brandenburg on the one hand, and Hamburg and Schleswig-Holstein on the other hand, who share the same authority. As a result, although there are 16 States, there are only 14 *Landesmedienanstalten*.

the FSM had to demonstrate it complies with a set of strict criteria and be approved by the KJM—hence the 'regulated' in 'regulated self-regulation'. In addition to overseeing its members' compliance with the interstate treaty, the FSM provides them with guidance, for instance when developing new tools or features, especially child safety or parental control tools. As a recognition of its role, it also has an observer status within the Global Online Safety Regulators Network, the global forum dedicated to supporting collaboration between online safety regulators.

§2 of the JMStV, which focuses on the scope of application of the treaty, specifies that its provisions 'shall also apply to providers who are not based in Germany [...], insofar as the services are intended for use in Germany'.[11] However, enforcing this rule has always been complex for German authorities. On the one hand, going after porn platforms who do not have a legal representation in the EU is close to an impossible mission. On the other hand, going after platforms established in other EU countries is overly complexified by the 'country of origin' principle enshrined in the AVMS Directive (as seen with the French case). In practice, German authorities first have to identify a postal address for the company—which is often burdensome—then send a formal letter and, if the company does not react, inform the regulator in the country of origin of the company and ask them to do something about it. If nothing further is done, German authorities must inform the European Commission of these proceedings and go to court in Germany, asking for an injunction or other measure. For a very long period, this heavy and time-consuming process discouraged German authorities from leveraging the extraterritorial scope of the JMStV. This was until a few years ago.

In a landmark case that spanned over four years, the Düsseldorf Administrative Court, in April 2023, dismissed lawsuits filed by porn platforms Pornhub, YouPorn, and Mydirtyhobby against the North Rhine-Westphalia State Media Authority. These three platforms, which all belonged to the MindGeek group (now Aylo), based in Cyprus, refused to implement age assurance mechanisms as ordered by the North Rhine-Westphalia State Media Authority and the KJM. With this decision, the Düsseldorf Administrative Court confirmed that the JMStV must be complied with, including by foreign platforms, and that it is to be enforced thoroughly. This, however, is in theory. In reality, the result of the proceedings was much more disappointing. The court indeed ordered that specific domain names be blocked for each of these companies. All these platforms had to do to circumvent the ban and continue their operations in Germany was change the subdomains of their websites. To make sure this does not happen again, a new version of the interstate treaty, which is to come into force in December 2025, will introduce additional provisions. Subdomains or 'mirror domains' will now also be covered by court decisions.

11 Own translation.

More recently, an expert commission was appointed by the German Federal Ministry for Education, Family Affairs, Senior Citizens, Women and Youth *(Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend* or BMBFSFJ*)*, tasked with developing a strategy to protect children and young people in the digital world. Deciding upon whether a social media ban should be put in place under a certain age and, if so, what the age threshold should be may fall within its mandate. In parallel, the BMBFSFJ is working on the development of its own age verification system, with a specific focus on data minimisation. In addition, just like the French Ministry for AI and Digital Affairs, it is pushing for the age assurance issue to be taken up at the EU level. Karin Prien, Federal Minister of Education, Family Affairs, Senior Citizens, Women and Youth, cosigned an opinion piece demanding an EU-wide implementation of mandatory age verification mechanisms across all social networks.

Lessons learned from the German experience

Germany demonstrates both the potential of structured, long-term age assurance governance and its limits in a fragmented EU legal order. In the end, even the most mature national system cannot succeed without coordinated EU-wide solutions.

- Germany has the deepest experience in Europe with enforcing age assurance, and its unique 'regulated self-regulation' model shows how state oversight and industry participation can combine to produce a large ecosystem of certified tools. This makes the country an important reference point for workable technical and institutional solutions.
- However, enforcement remains difficult when platforms are based abroad: the 'country of origin' principle and complex EU procedures have long discouraged German authorities from acting, and even landmark court victories (e.g. against MindGeek) were undermined by easy circumvention.
- Germany is now pushing the debate to the EU level, recognising that national enforcement alone is insufficient to protect minors in a borderless digital environment.

Growing calls for EU-wide age checks

In early June 2025, French president Emmanuel Macron announced his intention to have social media banned in France for under-15s 'in the coming months' if no progress was made at the EU level on this matter. Since then, the French Delegate Minister for AI and Digital Affairs, Clara Chappaz, has been on a crusade to rally other Member States to the cause. Cyprus, Denmark, Greece, Italy, Slovenia, and Spain soon joined forces in supporting the idea of having EU-wide age check mechanisms.

Just over two weeks after President Macron's announcement, 21 ministers from 13 Member States,[12] including BMBFSFJ's Karin Prien, as already mentioned, signed an op-ed asking to take decisive action 'now' to protect children online. For them, the current EU framework (they mention the BIK+ Strategy and the DSA) 'remains insufficient'. They ask for 'default privacy settings for children's accounts' on social media, 'calibrated recommender systems that prioritise explicit user feedback', and 'enhanced safety controls, including the ability for children to block or mute any user and protection from being added to group chats without their explicit consent'. **'Above all',** they go on, **'mandatory age verification mechanisms must be implemented across all social networks'.** These efforts seem to have been heard by the EU Executive to some extent.

On 14 July 2025, the European Commission released its guidelines on article 28(1) of the DSA, which detail examples of the concrete steps online platforms and search engines can undertake to comply with their obligation to 'put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service'. Sections 5 to 8 of the document 'set out the main measures that the Commission considers that such providers should put in place'. Under section 6, called 'Service design', more than 12 pages are dedicated to age assurance. Some political decision-makers and observers have interpreted these pages as a green light to Member States, allowing them to go ahead and adopt their own legal measures on age checks at national level. In a LinkedIn post, Caroline Stage Olsen, Minister of Digitalisation of Denmark, expressed how delighted she was that the European Commission had listened to the countries that 'have spoken out and pushed for better protection of children and young people on social media' and adopted 'more ambitious guidelines' than the draft ones that had been circulated. The Danish government 'will immediately begin work on this and investigate the possibility of an age limit', she added. Clara Chappaz, the French Delegate Minister for AI and Digital Affairs, shared her interpretation of the guidelines in a similar post. For her, the Commission's guidance 'paves the way for a ban on social media for children under 15 in national law'. 'Each Member State will be able to set a minimum age for accessing social media, and platforms will have to implement robust age verification measures', she observed, before applauding the fact that the guidelines 'also require age verification for pornographic websites'. Similarly to her Danish counterpart, she announced that the French government will do everything in its power to move forward with a ban on social media for under-15s in national law. The 'Age assurance under the DSA' section of this report shows that **these interpretations are a bit of a shortcut.**

12 Austria, Croatia, Cyprus, Denmark, France, Germany, Greece, Ireland, Italy, Luxemburg, Slovakia, Slovenia, and Spain.

Reacting to the publication of the guidelines, Danish socialist MEP and DSA rapporteur Christel Schaldemose was less enthusiastic. 'I still wish the European Commission would adopt a more ambitious stand on age verification for social media platforms', she told *Politico*. At the end of June, she had presented her draft report on the protection of minors online, in which she called on the European Commission to 'put forward recommendations for effective age assurance or age verification mechanisms to protect minors online, in accordance with the DSA, as a first step, and to present appropriate legislative measures if necessary'.

This is where we are at today: while some decision-makers are pushing for legal provisions on age assurance to be implemented at the Member State level, others (or sometimes even those same ones) are pushing for this to happen on an EU-wide level. **They all tend to ignore one thing: the existing EU digital rulebook already puts some obligations on online intermediaries when it comes to checking the age of their users. Before adding yet another layer to the existing legal *millefeuille*, these options deserve to be considered more thoroughly.**

The legal mandate: age assurance in the EU

As shown in this paper's overview of the EU-level legal framework aimed at protecting and empowering children online, several existing provisions oblige digital service providers to offer differentiated online experiences to minors than to adults. In other words, these measures mandate age assurance.

Age assurance under the GDPR

Recital 38 of the GDPR states that '[c]hildren merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data'. In addition, article 8, which deals with the conditions applicable to children's consent in relation to information society services, states that when consent is used as a legal basis to collect and process personal data, then:

- The entities collecting and processing that personal data, for instance social media platforms (Facebook, Instagram, Snapchat, TikTok, X ...), online gaming(-related) platforms (Discord, Epic Games, Steam, Roblox ...), or online video-sharing platforms (Dailymotion, Twitch, YouTube ...), must know if their users are above or below 16 (or 13, 14, or 15, depending on the Member State),[13] in order to establish whether collecting the consent of a legal guardian is necessary or not.
  This means that if they fail to do this check and collect and process the personal data of

13 This threshold was set at 13 in Belgium, Denmark, Finland, and Sweden, 14 in Austria, Italy, and Spain, and 15 in France and the Czech Republic. Other EU Member States are using the original 16 years old threshold set by the GDPR.

a person who is below the required age threshold, without obtaining the consent of a legal guardian, they are in breach of the GDPR.

- If it is found that a user is below the legally required age threshold, the entity collecting and processing the personal data must obtain the consent of a legal guardian. This means that if they fail to 'make reasonable efforts' to obtain this consent, or if they go ahead and collect and process the personal data without having obtained this consent, they are in breach of the GDPR.

An important legal gap is revealed here: the above is only valid if the legal basis used to collect and process personal data is the consent of the data subject. However, the data controllers may very well choose to opt for another legal basis to collect and process the personal data of minors, such as the execution of a contract, a legal obligation, or their own legitimate interests (see article 6 of the GDPR). **In fact, they almost never rely on consent,** as the empirical tests conducted as part of this report have revealed. In addition, in accordance with article 5(1)(b) of the GDPR, which sets out the principle of 'purpose limitation', each personal data collection activity must be tied to a specific, clearly defined purpose. As a result, online intermediaries usually rely on multiple legal bases depending on the precise purpose of each of their data collecting and processing activities. These purposes include the provision of the core service, ad personalisation, or safety and fraud prevention, for instance.

Age assurance under the AVMSD

The AVMS Directive, or AVMSD, regulates audiovisual media across the EU. **It applies to traditional TV broadcasters ('linear services'), on-demand services (such as streaming platforms, e.g. Netflix), and video-sharing platforms (e.g. YouTube) that fall within the jurisdiction of a Member State.** Its scope of application is thus broader than just EU-based AVMS providers. **Jurisdiction is based on the 'country of origin' principle:** a service is regulated by the Member State where the media service provider is established. Establishment depends on factors such as where the head office is located and where editorial decisions on the audiovisual content are taken (article 2 AVMSD). This means that non-EU companies are covered if they have an establishment in an EU Member State from which they direct their service into the EU market. For example, Netflix, whose European headquarters is in the Netherlands, falls under Dutch jurisdiction, while YouTube, operated in the EU by Google Ireland Ltd., falls under Irish jurisdiction—but both are subject to the AVMSD.

Article 6a of the AVMS Directive introduces specific protections for minors.

Article 6a of the AVMS Directive

1. Member States shall take appropriate measures to ensure that audiovisual media services provided by media service providers under their jurisdiction which may impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them. Such measures may include selecting the time of the broadcast, age verification tools or other technical measures. They shall be proportionate to the potential harm of the programme.

   The most harmful content, such as gratuitous violence and pornography, shall be subject to the strictest measures.

2. Personal data of minors collected or otherwise generated by media service providers pursuant to paragraph 1 shall not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.

Arguably, article 6a(1) leaves two options for audiovisual media service providers: either (option 1) they find a way to differentiate minors from adults to make sure that minors are gated from content that may impair their development or (option 2) they ban such content completely, including for adults. In addition, article 28b(3)(f) underlines that the measures AVMS providers may take to comply with article 6a(1) include 'establishing and operating age verification systems'.

Similarly, article 6a(2) leaves AVMS providers with the options of either (option 1) detecting minors in order to determine, for each given user, whether their personal data can be processed for commercial purposes or not, or (option 2) refraining from processing personal data for commercial processes altogether.

However, as already mentioned, unlike the GDPR or the DSA, the AVMSD is a directive—meaning that, to be applicable, it has to be transposed into the national law of EU Member States. This leaves Member States room for manoeuvre when it comes to indicating the precise steps that AVMS providers should take to comply with their obligations under articles 6a(1) and 6a(2). In their transpositions of the AVMSD, most EU countries (21 out of 27)[14] mention age verification as one of the measures to be implemented by video-sharing platform providers, if appropriate, in order to protect minors.[15]

Table 1: Overview of national transpositions of AVMSD rules regarding age verification
Countries with verbatim and substantially literal transpositions of Article 28b(3)(f) AVMSD

14 Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Portugal, Romania, Slovakia, Slovenia, and Spain.

15 Lacourt A., Munch E., Radel-Cormann J., AVMSDigest, Safe screens: Protecting minors online, European Audiovisual Observatory, Strasbourg, October 2024, p. 22.

BE(DE), BG, CY, CZ, DE, DK, ES, FR, GR, HR, HU, IE, IS, IT, LT, LU, MT, PT, RO, SI and SK		
Countries with broader or more detailed transpositions of Article 28b(3)(f) AVMSD VSP providers shall establish and operate:		
AT	**Federal Act on Audiovisual Media Services (AMD-G)** Consolidated 1st January 2021 -Art. § 39 (3)	Age verification systems or comparable access control measures must ensure that minors cannot usually follow the most harmful content, predominantly limited to the unreflective representation of sexual acts, or which contains parts of the program that are reduced to the representation of such content.
BE (FR)	**Decree on audiovisual media services and video-sharing services** 4 February 2021 - Art. 2.5-2	User-friendly, easy-to-use and efficient age verification system and introduce user-administered parental controls
BE (VL)	**Flemish community - Decree on radio and television broadcasting** Consolidated 1 December 2022 - Art. 176/6	Age verification systems for users of VSP services with respect to programmes, user-generated content and commercial communications which could be detrimental to the physical, mental or moral development of minors.

Source: This whole table is taken from Lacourt A., Munch E., Radel-Cormann J., AVMSDigest, Safe screens: Protecting minors online, European Audiovisual Observatory, Strasbourg, October 2024, p. 24.

Age assurance under the DSA

The Digital Services Act (DSA) is the most recent piece of EU regulation putting obligations on online platforms to protect minors specifically. Like the GDPR, it has an extraterritorial scope, meaning that it applies to providers established in the EU but also to providers outside the EU if they offer services to recipients in the EU (article 2(1)).

Article 28(2) of the DSA introduces a provision similar to that of article 6a(2) of the AVMS Directive: online platforms are not allowed to show ads based on personal data profiling if they know the user is a minor. **If they do not wish to refrain from using personal data to show targeted ads to their users altogether (which they most certainly do not), then they must find a way to know 'with reasonable certainty' if**

their users are minors or adults, which means they have to conduct some kind of age assurance. Here, '[w]ith reasonable certainty' suggests that self-declaration is not a reasonable option.

However, article 28(3) must also be taken into account here, as it states that compliance with article 28 'shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor'. Given that conducting age assurance without processing personal data is impossible, this paragraph seems to completely undermine the purpose of article 28(2), that is, unless we interpret it as meaning that the providers of online platforms themselves should not process additional personal data to determine the age of their users but that they may rely on third-party providers, who may be authorised to do so. Still, **this ambiguity does not help, and providers may very well (and most probably will) rely on it to avoid having to obtain sufficient certainty about the minority status of users targeted by ads.**

In addition, article 28(1) compels 'online platforms accessible to minors'—meaning the social media, marketplaces, and video-sharing platforms that are likely to be accessed by minors—to 'put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service'. To clarify this rather vague wording, the European Commission issued specific guidelines on 14 July 2025. This guidance document provides insights to providers of online platforms accessible to minors on:

- how to determine whether to put in place access restrictions supported by age assurance measures or not (6.1.2);
- where applicable, which age assurance method to use (6.1.3); and
- how to assess the appropriateness and proportionality of any age assurance method (6.1.4).

With regards to this last point, **the Commission observes that age assurance methods used to protect minors online should be accurate, reliable, robust, nonintrusive, and nondiscriminatory.**

Regarding the type of age assurance method to use when deemed necessary, **the EU executive 'considers the use of age verification**[16] **methods an appropriate and proportionate measure to ensure a high level of privacy, safety, and security of minors'**:

- a. [w]here applicable Union or national law prescribes a minimum age to access certain

16 '[A] system that relies on physical identifiers or verified sources of identification that provide a high degree of certainty in determining the age of a user.'

products or services offered and/or displayed in any way on the online platform (e.g. sale of alcohol or tobacco, access to pornographic content, access to gambling platforms).

- b. [w]here, due to identified risks to minors, the terms and conditions or any other contractual obligations of the service require a user to be 18 years or older to access the service even if there is no formal age requirement established by law.
- c. [w]here national law, in accordance with Union law, prescribes a minimum age to access certain products or services offered and/or displayed in any way on an online platform, including specifically defined categories of online social media services.
- d. [a]ny other circumstances in which the provider of an online platform accessible to minors has identified high risks to minors' privacy, safety, or security, including content risks as well as contact risks (e.g. arising from features such as live chat, image/video sharing, anonymous messaging), where these risks cannot be mitigated as effectively by other less intrusive measures as they can by access restrictions supported by age verification.

While most experts usually agree with the European Commission on point a, the other three points are more subject to disagreements.

In the most recent public debates and policy developments, point c has become the main focus of attention. As mentioned earlier, some decision-makers, such as France's and Denmark's ministers for digital affairs, were quick to interpret this paragraph as giving a green light to Member States to adopt their own national level measures on age verification. However, one detail in the Commission's wording should not be overlooked here. National law may prescribe a minimum age to access certain products or services but only if this is done 'in accordance with Union law'. If anything, the French experience, with its law introducing an age of digital majority at 15 to access social media platforms, has shown that the European Commission considers these kinds of initiatives as clashing with the DSA. **Here, again, the ambiguity risks leading to lengthy legal procedures involving the Court of Justice of the EU, further delaying implementation and enforcement.**

In addition to age verification, the article 28 guidelines indicate that **age estimation**[17] may also be an appropriate and proportionate way to conduct age assurance under certain circumstances. An example is when a platform's rules (e.g. its terms and conditions) say that users must be above a minimum age—but that age is set below 18—in order to use the service. This is the case with the majority of platforms that are widely used by children, who typically set this threshold at 13 years old.

Although the EU Executive indicated that these guidelines may 'be considered a

17 Methods that allow a provider to establish that a user is likely to be of a certain age, to fall within a certain age range, or to be over or under a certain age, for example using behavioural/contextual signals (e.g. browsing habits, language use, or interaction patterns) or facial age estimation based on artificial intelligence.

significant and meaningful benchmark on which the Commission as well as digital services coordinators and competent authorities will base itself when applying article 28(1) of [the DSA] and determining the compliance of providers of online platforms accessible to minors with that provision', they are not legally enforceable: only the DSA in itself is. This means that platforms could very well choose not to follow them strictly. It also means that they could follow them precisely and still be considered noncompliant with the DSA or other EU rules.

The compliance gap: age assurance in practice

To assess whether online intermediaries comply with age assurance obligations under the AVMSD, GDPR, and DSA, I have conducted tests[18] on the social media, video-sharing, and gaming services that are most commonly used by under-16 users in the EU: Discord, Fortnite, Instagram, Roblox, Snapchat, TikTok, Twitch, and YouTube. The aim was to assess whether these platforms check the age of new users when they create their accounts and whether they make sure to obtain the consent of a legal guardian if the user is underage.

To conduct these tests, I created avatar accounts using the birth date of a 14-year-old and, if encountering some kind of block (e.g. impossible to create an account due to self-declaring being below a certain age threshold), I declared being 16 or 18, depending on the case (see details in the table below). The results speak for themselves**: all of the online platforms that are most commonly used by minors in the EU rely on self-declaration to check the age of a user when creating an account.** However, as observed by the 5Rights Foundation in a 2021 report, '[s]elf-declaration is often referred to as "tick box" age assurance and is associated with the current failure to truly establish the age of children online. It requires a user only to enter their birthdate, or to tick a box that asks if they meet the minimum age of use'.[19]

As a result, I was able to create accounts on all of these platforms using only self-declaration and without encountering any type of more robust age check or parental consent requirements (except for YouTube, which put in place a parental consent tool but one which can easily be circumvented by creating a Google account using the (self-declared) birthdate of a person that is over 18). In addition, some of these apps and websites, such as Fortnite, Instagram, Snapchat, Twitch, TikTok, and YouTube, ask for additional, potentially identifying personal data such as the name, surname, and gender of the individual.

18 These tests were all conducted using a France-based IP address on 29 July 2025.
19 5Rights Foundation (2021), *op. cit.*

Table 2: Results of compliance checks with age assurance and parental consent obligations under EU law

Name of service	Type of age check	Type of parental consent check
Discord[20]	**Self-declaration** (user must enter a birth date). By indicating the birth date of a 16-year-old, I was able to create an account. A verification link is sent by email.	**None.**
Fortnite (Epic Games)[21]	**Self-declaration** (user must enter a birth date). By indicating the birth date of a 16-year-old, I was able to create an account. In that case, the service also asks for a name and surname. A verification code is sent by email. By entering the birth date of a 14-year-old, I was also able to create an account, but it had limited functionality (e.g. communication with other players via voice chat or direct messages and in-game purchases were disabled).	**None** if the birth date of a 16-year-old is indicated. If the birth date of a 14-year-old is indicated, the platform asks for the email address of a legal guardian. The person behind the indicated email address then receives an email with a link to approve or refuse Epic Games' data processing practices, its terms of service, and its privacy policy. However, even before the legal guardian receives the email and clicks on the link, the account is created and can be used by the minor, although with limited functionality.
Instagram[22]	**Self-declaration** (user must enter a birth date). By indicating the birth date of a 16-year-old, I was able to create an account. The service also asks for a name and surname. A verification code is sent by email.	**None.**
Roblox[23]	**Self-declaration** (user must enter a birth	**None.**

	date). I was able to create an account without encountering any kind of age check, despite the birth date entered being that of a 14-year-old. No email address or phone number is needed. A username is created (Roblox specifically asks users not to use their real name). Access to voice chat can be unlocked by registering a phone number. In that case, a verification code is sent to the indicated phone number.	
Snapchat[24]	**Self-declaration** (user must enter a birth date). I was able to create an account without encountering any kind of age check, despite the birth date entered being that of a 14-year-old. The service also asks for a name and surname. A verification code is sent by email.	**None.**
TikTok[25]	**Self-declaration** (user must enter a birth date). I was able to create an account without encountering any kind of age check, despite the birth date entered being that of a 14-year-old.	**None.**

20 Test conducted on 29 July 2025. Site tested: https://www.discord.com
21 Test conducted on 29 July 2025. Site tested: https://www.fortnite.com
22 Test conducted on 29 July 2025. Site tested: https://www.intagram.com
23 Test conducted on 29 July 2025. Site tested: https://www.roblox.com/fr

	The service also asks for a name and surname. A verification code is sent by email.	
Twitch	Self-declaration (user must enter a birth date). I was able to create an account without encountering any kind of age check, despite the birth date entered being that of a 14-year-old. The service also asks for a name and surname. A verification code is sent by email.	**None.**
YouTube[26]	Google makes it impossible to create a YouTube account without having it connected to a Google account. If the Google account used to access YouTube belongs to a 14-year-old, some kind of parental consent is implemented (see right cell).	If the Google account used to create a YouTube account belongs to a 14-year-old, the legal guardian receives an **email** to approve the creation of the account and set basic settings (which version of YouTube Kids the minor can access, can they search for videos or not, etc.). Without this approval, the minor cannot access a YouTube account.
	It is, however, possible to create a Google account indicating the date of birth of an adult, as **self-declaration** is used without any further checks. Only a phone number or email address is required (a verification code is sent). In that case, the service also asks for	**None** if the Google account used to create a YouTube account supposedly belongs to an adult (which is not checked in any way other than through self-declaration, by indicating a date of birth).

24 Test conducted on 29 July 2025. Site tested: https://www.snapchat.com
25 Test conducted on 29 July 2025. Site tested: https://www.tiktok.com/fr/

	the name (mandatory), surname (optional), and gender (mandatory) of the person.	

These preliminary findings require further investigation over a longer period of time.[27] **Still, they show that the tested platforms do not efficiently check the age of their users at registration and so do not necessarily offer a differentiated online experience to minors from the outset (e.g. not using their personal data for targeted advertising purposes, as mandated by the AVMSD and DSA).**

They also appear to be in breach of contract law in most (possibly all) EU Member States. As explained in the 'Age assurance under the GDPR' section of this report, online intermediaries processing personal data must check the age of their data subjects only if the legal basis used to justify the specific data processing activity is consent (article 8(1) of the GDPR). Among the platforms I tested, none use this legal basis for the purpose of providing their core service. Instead, they rely on the 'performance of a contract' legal basis. In other words, they consider that 'processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract' (article 6(1)(b) of the GDPR). As a result, they do not have to check whether the data subject is old enough to consent to the data processing under the GDPR.

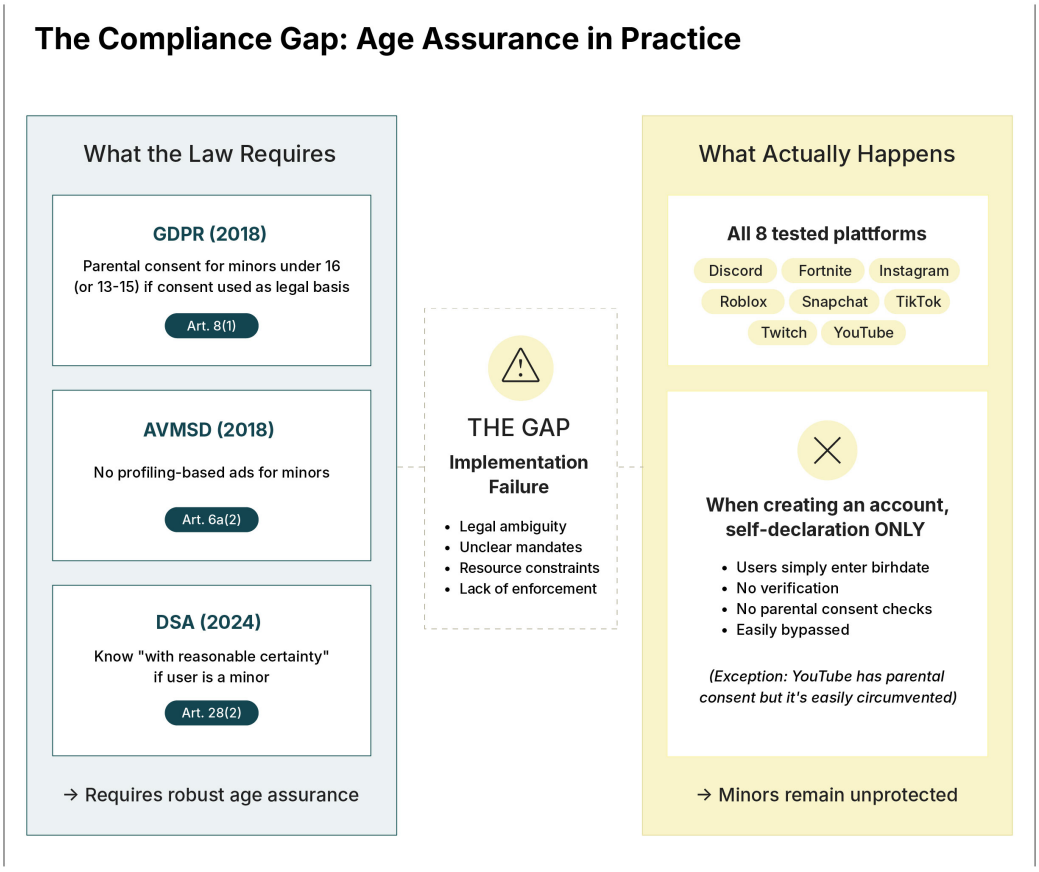
However, this does not exempt them from ensuring that the data subject, as a consumer, is old enough to legally enter into a contract—which depends on the applicable contract law of the Member State where the person resides. In most EU countries, minors below the age of 18 do not have the legal capacity to enter into a contract, with some exceptions, for instance if a legal representative or guardian has given their consent. As the results of our tests have shown, **none of the studied platforms effectively check the age of their users when they create an account, and none of them have implemented effective parental consent tools. They thus have no way of knowing whether the contracts their data subjects are entering into with them are valid or not.** The validity of the contract—and thus the validity of processing under article 6(1)(b) of the GDPR—depends on whether the contract is legally binding under national law. If the user is a minor and the contract is voidable or invalid without parental consent, then the data processing activity is illegal.

Moreover, as indicated in their own rules (generally their terms and conditions or

26 Test conducted on 29 July 2025. Site tested: https://www.youtube.com

27 Some platforms may require users to prove their age at a later stage if, after the person has used the service for a while, the platform has reasons to believe they may be underage (e.g. based on the content or accounts they engage with).

privacy policies), all of the tested platforms use consent as a legal basis for at least one specific purpose: personalised advertising/marketing emails/optional cookies. It would be worth investigating this further to assess if and how these online intermediaries make sure that their data subjects are old enough to autonomously consent to third-party cookies, for instance. Based on the results of this investigation, it could be assessed whether they comply with article 8(1) of the GDPR.



Avenues for better enforcement of age assurance and online child protection across the EU

As demonstrated, **all of the platforms that are most used by children and teenagers in the EU appear to be (at least partially) in breach of the GDPR, AVMSD, and/or DSA.**[28] This section aims to provide insights to EU and national decision makers, responsible authorities, online services, NGOs and civil society on how to improve enforcement of these already existing rules.

Who does what?

To clarify the mandate of responsible authorities, Appendix 2 identifies, for each of the possible breaches of specific GDPR, AVMSD, and DSA provisions mandating age assurance, who is the entity responsible for enforcement within the EU. Although this basic first step may seem simple, this research has shown that it is not always the case. This exercise is in fact very informative.

First of all, **it reveals how complex it can be, due to overlaps in these pieces of legislation, to find the responsible authority.** This is particularly true for article 6a(2) of the AVMSD, dealing with the processing of minors' personal data for targeted advertising purposes, whose enforcement potentially involves both media regulators and data protection authorities. The same goes for enforcement of article 28(2) of the DSA, dealing with the same obligation, which generally requires the cooperation of digital services coordinators (DSCs) with data protection authorities (DPAs). Depending on the Member State, the way in which the cooperation between these actors and their respective responsibilities is organised may vary. A tricky example is that of Twitch. Since it has designated Twitch Interactive Germany GmbH as its legal representative in the EU, it falls under the jurisdiction of the German DSC at the BNetzA when it comes to its overall compliance with the DSA. However, for article 28(2) of the text, *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (BfDI), the German Federal Commissioner for Data Protection and Freedom of Information, is the only authority in charge of enforcement.

It also reveals how, due to the 'country of origin' principle enshrined in the AVMSD and to the obligations under article 13 of the DSA, the responsibility for enforcing these provisions mainly lies with a handful of actors: essentially the DSCs and DPAs of Ireland and the Netherlands. This is often described as a bottleneck situation, as a very small number of regulators potentially have to deal with a lot of substantial cases. In part to cope with this situation, Ireland has chosen to bring the oversight powers of the DSA and AVMSD under one single, newly created authority, *Coimisiún na Meán* (CNAM), the media regulator.

The GDPR adds another level of complexity here, as it does not rely on the 'country of origin' principle but on a 'one-stop shop' mechanism: the 'lead supervisory authority' is the DPA of the Member State where the data controller or processor is established in the EU.[29] Not only is this authority 'competent to act as lead

28 This would need to be investigated further by comparing to other, less successful platforms used by minors; however, the reason why these platforms are popular with children and teenagers may be because they do not effectively implement age assurance mechanisms.

supervisory authority for the cross-border processing carried out by that controller or processor' (article 56(1) of the GDPR) but it also coordinates cross-border cases with other relevant DPAs when needed (article 60 of the GDPR). In addition, any other national DPA may decide to launch an investigation into a company that is under the jurisdiction of the lead authority, for instance if its citizens are specifically affected (article 56(2) of the GDPR) and if the lead authority agrees (article 56(5) of the GDPR). The European Data Protection Board (EDPB) may step in if authorities disagree. As a result of this mechanism, virtually any EU-based DPA may be competent to enforce articles 6(1)(b) and 8 of the GDPR on a given actor.

It is partly to avoid this bottleneck situation that the European Commission has chosen to have a more active role in overseeing the DSA, by taking over enforcement for VLOPs, such as Instagram, Snapchat, TikTok, and YouTube. Although it has launched some investigations under the DSA already, specifically around minors' protection measures—concerning Instagram and TikTok for instance—it is still too early to assess whether this greater role for the Commission will lead to improved enforcement.

Obstacles to enforcement efficiency ...

When it comes to the enforcement of existing age assurance rules in the EU, this research reveals multiple reasons behind the apparent lack of effectiveness.

First, as we have just seen, **the juxtaposition of rules, each dealing with a specific aspect of age assurance in the context of online child protection, makes it difficult to identify who is responsible for what.** Hopefully, the table presented in Appendix 2 and the above comments can be seen as a modest contribution to overcoming this difficulty.

Second, **this juxtaposition of rules introduces a need for sectoral regulators from different backgrounds (e.g. under the AVMSD and the DSA) and from different countries (e.g. under the GDPR) to work together.** Things are a bit different for data protection authorities, who have been used to working together within the 'G29'—which later became the EDPB when the GDPR entered into force—since 1998. As a result of this mechanism, most EU-based DPAs[30] have more than 25 years of experience working together on cases. However, when it comes to

29 Or that of the country where it has its main establishment, if it is established in more than one EU country. There is, however, an exception to that rule: article 56, which establishes the role of the lead supervisory authority, does not apply if the processing is necessary for compliance with a legal obligation to which the controller is subject or if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In that case, each supervisory authority is competent in the territory of its own Member State, and the lead supervisory authority (if different) cannot intervene.

30 Not all of them, since some Member States joined the Union after 1995.

collaboration between media regulators and data protection authorities, as required by the AVMSD, or between DSCs and data protection authorities, as required by the DSA, things are not so simple. Differences in administrative culture, (in)dependence status, and methodologies, as well as technical and legal challenges, all constitute obstacles to this cooperation.[31] This is all the more vivid under the DSA, with the specific role of the DSCs, who themselves may be a telecoms regulator, a media regulator, a competition authority, a consumer protection authority, and so on, depending on the Member State (full list available here). Not only do they have to coordinate at the EU level with their counterparts, within the European Board for Digital Services, but they also must coordinate at the national level with the other authorities that are competent under the DSA for sector-specific matters. In France, for instance, Arcom, the media regulator and designated DSC, must coordinate with the *Commission nationale de l'informatique et des libertés* (CNIL), the country's DPA, and with the *Direction générale de la concurrence, de la consommation et de la répression des fraudes* (DGCCRF), a consumer protection administration placed under the Ministry of the Economy. Similarly, in Germany, the DSC is the competent authority for most parts of national DSA enforcement, but key elements of the DSA—youth protection prominently among them—are supposed to be enforced by other competent authorities, namely, the *Landesmedienanstalten* (State media authorities), the Federal Commissioner for Data Protection and Freedom of Information (BfDI), and the Federal Agency for Child and Youth Protection in the Media (BzKJ). Efficient cooperation mechanisms at the EU and national levels will take years to take shape, especially for smaller countries in which competent authorities have scarce resources.

Third, and this is very much linked to the previous point, **enforcement authorities lack the human and financial resources both to carry out investigations and make sure the rules they are entrusted to enforce are respected and to engage in cooperation efforts with other entities.** In its last Annual DSA Report, KommAustria, Austria's DSC, notes the difficulty in hiring competent staff: 'The implementation of the DSA requires employees with specialised knowledge in the field of digital services, some of whom are currently in high demand on the labour market.'[32] On the coordination between DSCs at the EU level, it also notes that its workload related to the Board of Digital Services turned out to be 'significantly larger' than initially expected.[33] In addition, a recent report by the Global Digital Human Rights Network observes that 'Czechia noted that its authority lacks staff to perform the tasks prescribed by the DSA', and that the other EU Member States covered in the study (Austria, Cyprus, Finland, Germany, Italy, and Portugal) 'have

31 For more on this, see: Renaissance Numérique (2025), 'For an Effective Interregulation in the Digital Sphere', 44 pp.
32 KommAustria (2025). 'Jahresbericht des österreichischen Koordinators für digitale Dienste 2024', p. 21. *Own translation.*
33 *Ibid.*, p. 22.

indicated that staffing as well as limited financial resources for regulatory authorities in general might hamper effective enforcement for the DSA'.[34] **This point, however, is to be put in perspective with the findings put forward in this paper, as even very basic testing already reveals GDPR, AVMSD, and DSA breaches.**

However, because their resources are not infinite, enforcement authorities must prioritise certain investigations over others and are *de facto* not in a position to address all situations putting underage users at risk. The example of France is typical. For years, legislators have been passing laws, NGOs have been going to court, and Arcom has been engaged in efforts aimed at forcing online platforms hosting adult content to implement age check mechanisms. After more than half a decade of actions, the vast majority of concerned actors still do not comply with their legal obligations. In this context, it may be difficult for the regulator to justify going after social media platforms 'just because' they do not check whether their users are old enough or not to sign a contract. While making pornographic content available to minors constitutes a criminal offence, it is not forbidden for minors to create an account on a social media platform as long as, under national contract law, they are old enough to enter into a contract or their legal guardian has agreed to it.[35]

… and how to overcome them: recommendations to key players

It is still too early to say if the legal provisions that were adopted in 2024—in particular Article 28 of the Digital Services Act (DSA) and its accompanying guidelines, both dealing specifically with the protection of minors online—will be effective. However, they introduce an interesting dynamic, encouraging Member States' authorities to work closer together on those issues and to tackle the question of age assurance at the EU level. Assessing whether this is more efficient than the mechanisms that were in place until now will require some testing and learning.

This does not mean that nothing can be done straight away to better protect children and teenagers online. The below recommendations stem from the legal analysis, empirical compliance tests results, and challenges to enforcement effectiveness exposed above. They are meant to guide policymakers and regulators at both the national and EU levels on the levers of actions available to them if they want to act now, based on the legal and regulatory tools that are already in place. Looking to the

34 Global Digital Human Rights Network (2024), 'Do the New European Rules on Digital Services Effectively Ensure Human Rights on Platforms? Assessment Models for States', pp. 12-13.

35 That is, if the legal basis used by the platform to provide the core service is the performance of a contract, which is systematically the case for the online platforms studied in this report.

future, these recommendations also suggest options to better protect young internet users, other than by overly focusing on age assurance, as is the case at the moment. To some extent, they also provide guidance to civil society organisations and NGOs working in the field in terms of how to best assist decision-makers, supervisory authorities, and society at large. Finally, they include advice addressed to digital service providers themselves. As much as possible, these recommendations tend to be technically feasible and actionable in the short to medium term.

Recommendations to EU-level policymakers

- Before contemplating any new legal initiative, **take stock of the binding provisions that already mandate age assurance at the EU level and assess their efficiency.**
- **Provide guidance to national authorities** on how the age assurance provisions enshrined in the AVMSD, GDPR, and DSA overlap and how best to leverage them to hold online intermediaries accountable.
- **Think twice before incorporating age assurance into hard law at the EU level.**
- An EU-wide ban under a certain age may be acceptable concerning access to pornographic content, gambling platforms, or the sale of alcohol. However, although the age checks ecosystem has greatly matured in recent years, the French case shows that age assurance tools remain perfectible and must be independently audited, especially in terms of privacy preservation. The German case, with its 'regulated self-regulation' model, may be able to provide best practices in this regard. As to imposing a minimum age to access social media or video sharing and streaming platforms, this would not in itself help children, as this would simply delay their exposure to harmful or illegal content.

Recommendations to national policymakers

- To avoid fragmentation of the EU's Digital Single Market, as well as lengthy and costly legal proceedings, **tackle the issue of online child protection at the EU level.** Legislators in some countries, such as France and Denmark, are contemplating passing laws to ban social media access for persons under a certain age or to oversee the activities of online influencers. As much as possible, these discussions should take place within the EU decision-making sphere.
- **Expend the resources available to national independent regulatory authorities**, both in terms of allocated budget and full-time equivalents.
  This may be hard to implement in the short to medium term, at a time when most EU Member States are undergoing budgetary constraints. This may mean refraining from adopting additional legislation regulating online platforms and focusing on providing the means to enforce existing ones.

Recommendations to the European Commission with regards to its regulator role

- **Conclude, in a timely manner, investigations into Meta (Instagram and Facebook) and TikTok under article 28(1) of the DSA,** without shying away from the Commission's responsibility in the face of mounting pressure from Big Tech companies and the Trump administration.

- **Contemplate opening additional legal proceedings** to assess whether the digital services under its oversight (VLOPs and VLOSEs) are complying with article 28(2) of the DSA, and whether other intermediaries than Meta and TikTok may be breaching article 28(1).

Recommendations to national authorities and regulators

These recommendations apply to national authorities and regulators — provided they have the necessary resources to act.

- **Engage in cross-border cooperation as much as possible,** on a case-by-case basis, but also **strengthen cooperation between the European Regulators Group for Audiovisual Media Services (ERGA), the European Data Protection Board (EDPB), and the European Board for Digital Services.**
- **Contemplate opening investigations against the online intermediaries that fall under their jurisdiction** when it comes to complying with child protection rules under the DSA, AVMSD, and GDPR (see Appendix 2).

Recommendations to CSOs and NGOs

- To assist regulators and decision-makers, **keep monitoring and publicly report on compliance of digital platforms with child protection legal provisions and bring strategic litigation where companies consistently fail to protect minors' rights online.**
- **Advocate against simplistic 'tick-the-box' approaches** to compliance that do not truly safeguard children.

Recommendations to digital service providers

- **Implement as soon as possible the guidelines of the European Commission on article 28 of the DSA.** In particular, these services should be transparent about the measures they take, to allow auditing organisations, researchers, NGOs, and civil society at large to assess whether these are effective and compatible with EU law, while respecting fundamental rights and freedoms.
- **Consider applying some of the recommendations from the European Commission's DSA article 28 guidelines to all accounts, irrespective of the age of the user,** to '[e]nsure that privacy, safety and security by design principles are consistently applied'. This includes, for instance, setting accounts as private by default, turning off the default autoplay of videos and hosting live streams, turning off push notifications, and ensuring that recommender systems prioritise explicit user-provided signals to determine the content displayed.

Conclusion

Over the past two decades, the EU has assembled a body of rules aimed at protecting children in the digital sphere. The GDPR, AVMSD, DSA and complementary strategies such as BIK+ form a dense regulatory fabric that acknowledges and aims

to address the specific vulnerabilities of children online. Member States, too, have experimented with ambitious national measures, ranging from France's SREN Act to Germany's *Jugendmedienschutz-Staatsvertrag* and 'regulated self-regulation' approach. Despite these initiatives, the findings of this paper show a persistent reality: children remain insufficiently protected, and the gap between legal obligations and the everyday practices of online platforms is wide.

Age assurance sits at the centre of this paradox. On paper, it is one of the indispensable gateways to enforcing many existing obligations, from limiting exposure to harmful content to banning targeted advertising based on minors' data. In practice, however, the overwhelming reliance on self-declaration, the lack of tools that are both effective and rights-preserving, the absence of robust parental consent mechanisms, and the lack of systematic enforcement render age assurance one of the weakest links in the chain of online child protection. National experiments demonstrate both the potential and the limits of acting alone: France's attempts collide with EU competences and risk fragmentation, while Germany's unique model of 'regulated self-regulation' has yielded a pool of certified tools but still struggles against the extraterritorial nature of digital platforms.

This implementation gap is not only the result of inadequate technical solutions. It is symptomatic of deeper challenges: regulatory overlaps that blur accountability, enforcement authorities with insufficient resources, and legal ambiguities that platforms exploit to avoid compliance. The result is a 'tick-the-box' culture of compliance that satisfies procedural requirements without addressing substantive risks to children's safety, privacy, and well-being. If the EU continues down this path, the danger is that child protection becomes a bureaucratic exercise rather than a lived reality for young users.

The way forward requires shifting perspective. Age assurance may have a role to play, especially in contexts where access to certain types of content (e.g. pornography, gambling, and alcohol sales) is legally prohibited under a given age. However, it cannot, and should not, be treated as a silver bullet. One thing it does not allow, for instance, is to ensure that there are safe spaces where children and teenagers can communicate with peers without the fear that adults can join in. Protecting children online demands a more holistic approach: One that embeds safety and privacy by design and by default into the core architecture of platforms, rather than outsourcing responsibility to parents and carers or to after-the-fact checks. One that addresses systemic risks and business models, recognising that the attention economy and engagement-maximising design features are at the root of many harms faced by minors. One that invests in digital literacy and empowerment for all age groups, equipping users to understand recommender systems, monetisation models, and their own rights, and enabling parents to better guide their children's online experiences. One that extends protection beyond minors, by

ensuring that design practices that harm children are not applied to adults either, thereby promoting a safer and more rights-respecting digital environment for everyone.

Europe does not lack the legal tools to protect minors online: it lacks effective implementation and a holistic vision. Rather than layering yet another regulation on top of an already complex framework, the EU should make the existing rules work while redirecting attention to the underlying drivers of online harm. The European Commission's guidelines on measures to ensure a high level of privacy, safety, and security for minors online provide a good baseline in this regard. If enforcement is strengthened, the systemic risks addressed, and user empowerment prioritised, the EU can move closer to its ambition of creating a digital environment that is safe, empowering, and respectful of rights—not only for children, but for all.

Appendices

Appendix 1—Overview of the rules safeguarding minors online in the EU

This overview, last updated on 21/09/2025, aims to be as comprehensive as possible. If you spot any inaccuracies or missing points, do not hesitate to contact the author.

The rules safeguarding minors online in the EU go from international treaties whose main focus is not children in digital environments, but which do include relevant provisions, such as the United Nations Convention on the Rights of the Child, to more tailored texts such as the European Commission's Proposal for a regulation laying down rules to prevent and combat child sexual abuse. Some focus on the protection of children's personal data, others on shielding them from certain content, services, and products or on strengthening their rights. Most importantly, however, some of these texts are legally binding and enforceable by authorities, such as the EU Digital Services Act (DSA), while others provide non-mandatory roadmaps, such as the European Declaration on Digital Rights and Principles for the Digital Decade.

Binding instruments

At the EU level, the main pieces of legislation dealing with online child safety and empowerment are:

- The **General Data Protection Regulation (GDPR),** which is applicable since 2018, in particular articles 6(1)(f), 8(1), and 12(1). *See below for details.*

- The **Audiovisual Media Services Directive (AVMSD),** which first entered into force in 2010 and was revised in 2018, in particular articles 6a(1), 6a(2), 6a(3), 9(1)(e), 9(1)(g), 28b(1)(a), and 28(b)(3). *See below for details.*
- The **Digital Services Act (DSA)**, which entered into force in 2024, especially articles 14(3), 25(1)(j), 28, 34(1)(d), and 44(1)(j). *See below for details.*
- The **Artificial Intelligence (AI) Act**, which entered into force in 2024, especially articles 5(1)(b) and 9(8). *See below for details*.

In addition to these key pieces of legislation, in May 2022 the European Commission proposed a Regulation laying down rules to prevent and combat child sexual abuse, with key provisions focusing on child sexual abuse material (CSAM) online. The proposed rules include an obligation for digital service providers to detect, report, and remove CSAM on their services. Three years later, however, no common position has been reached at the Council of the EU, and this proposal is at a standstill.[36]

The GDPR

GDPR provisions dealing with minors in digital environments:

Concept	Article	Explanation
Legal basis for processing the personal data of minors	6(1)(f)	When legitimate interest is used as a legal basis for processing the personal data of a minor, specific attention should be given to the balance between this legitimate interest and the minor's fundamental rights and freedoms.[37]
Autonomous consent[38] of minors	8(1)	Minors over the age of 16 can give their own consent to certain personal data processing operations based on non-contractual consent (e.g. they can legally decide on their own to accept cookies to consult a website, to opt for a public or private profile on a social network, etc.). Member States are allowed to adopt specific national measures to place this age between 13 and 16.
Dual consent of minors and legal guardians	8(1)	When the minor is under the age of 16, processing is only lawful if consent is given jointly by the minor concerned and the person or persons with parental authority over the minor. Member States are allowed to adopt specific national measures to place this age between 13 and 16.
Empowerment of minors	12(1)	Minors must be able to control the data that concerns them, and the information provided must be appropriate.

36 Because this paper focuses on measures that have been adopted and are already in force, this regulation has been left out of the scope of analysis. For similar reasons, the provisions enshrined in the temporary derogation from the ePrivacy Directive—which allows some digital service providers to use technologies to detect, report, and remove CSAM on their services, until the above-mentioned 'CSAM Regulation' is adopted—are not covered here.

37 As specified in the EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, this balancing exercise should ensure that the best interest of the child is the primary consideration, in accordance with the EU's Charter of Fundamental Rights and the United Nation's Convention on the Rights of the Child.

Although article 25 of the GDPR (on data protection by design and by default) does not specifically deal with children, it is worth mentioning that the European Data Protection Board (EDPB)[39]'s Guidelines 4/2019—which are not binding—specify that the principles of by default and by design data protection must be adapted to children.

The AVMSD

AVMSD provisions dealing with minors in digital environments:

Concept	Article	Explanation
Targeting of minors with ads based on profiling	6a(2)	Personal data of minors collected or otherwise generated by media service providers shall not be processed for commercial purposes, such as direct marketing, profiling, and behaviourally targeted advertising.
	6a(1)	Content that may impair the physical, mental, or moral development of minors must only be made available in such a way as to ensure that minors will not normally hear or see them. Such measures may include selecting the time of the broadcast, age verification tools, or other technical measures. They shall be proportionate to the potential harm of the programme. The most harmful content, such as gratuitous violence and pornography, shall be subject to the strictest measures.
	6a(3)	Media service providers must provide sufficient information to viewers about content that may impair the physical, mental, or moral development of minors. For this purpose, they shall use a system describing the potentially harmful nature of the content of an audiovisual media service.
	28b(1)(a) and 28b(3)	Video-sharing platform providers must take appropriate measures to protect minors from programmes, user-generated videos, and audiovisual commercial communications that may impair the physical, mental, or moral development of minors. These measures shall consist of, as appropriate *(N.B. this list is not exhaustive)*: · including this requirement in their terms & conditions; · establishing and operating age verification systems; · providing for parental control systems; · providing for effective media literacy measures and tools and raising users' awareness of those measures and tools.

Unlike the GDPR, DSA, or AI Act, the AVMSD is a directive, not a regulation. Consequently, it is binding 'only as to the result to be achieved', granting Member States the power and flexibility to 'choose the form and methods for achieving the specified result'.[40] While regulations are directly applicable across all Member

38 As specified in EDPB Guidelines 05/2020 on consent under Regulation 2016/679, consent processes must be adapted to minors.
39 The EU-level body which gathers all the Members States' data protection authorities.

States, transposition into national law is required before directives become applicable. Although the deadline for transposing the AVMSD into national law was 19 September 2020, only five countries transposed it on time. As a result, in November of that year, the European Commission launched infringement proceedings against 23 Member States. In May 2022, Czechia, Ireland, Romania, Slovakia, and Spain were referred to the Court of Justice of the European Union (CJEU) for noncompliance. As of December 2024, all Member States had finally completed full implementation, more than four years after the deadline. **This delay is the perfect illustration of how having rules on paper may be nice, but it does not necessarily mean they are immediately enforceable. To avoid such delays, as well as regulatory fragmentation, the EU has been using regulations rather than directives as its main legal instruments in the area of tech policy these last few years (e.g. Digital Markets Act, Digital Services Act, Data Act, Data Governance Act, AI Act, etc.).**

The DSA

DSA provisions dealing with minors in digital environments:

Concept	Article or recital	Explanation
Targeting of minors with ads based on profiling	Art. 28(2)	Providers of online platforms shall not present advertisements on their interface based on profiling using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor.
	Art. 28(3)	Compliance with the obligations set out in [Art. 28(2)] shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor.
Understandable terms and conditions	Art. 14(3)	Where an intermediary service is primarily directed at minors or is predominantly used by them, the provider of that intermediary service shall explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand.
Definition of an online platform that is 'accessible to minors'	Rec. 71	An online platform can be considered to be accessible to minors when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes.

40 Rupp. C. (2024), 'Navigating the EU Cybersecurity Policy Ecosystem - A Comprehensive Overview of Legislation, Policies and Actors'.

Risk assessments	Rec. 81	When assessing risks to the rights of the child, providers of very large online platforms and of very large online search engines should consider, for example, how easy it is for minors to understand the design and functioning of the service, as well as how minors can be exposed through their service to content that may impair minors' health or physical, mental, or moral development. Such risks may arise, for example, in relation to the design of online interfaces that intentionally or unintentionally exploit the weaknesses and inexperience of minors or that may cause addictive behaviour.
Best interests of the child	Rec. 89	Providers of very large online platforms and of very large online search engines should take into account the best interests of minors in taking measures such as adapting the design of their service and their online interface, especially when their services are aimed at minors or predominantly used by them. They should ensure that their services are organised in a way that allows minors to easily access mechanisms provided for in this Regulation, where applicable, including notice and action and complaint mechanisms. They should also take measures to protect minors from content that may impair their physical, mental, or moral development and provide tools that enable conditional access to such information.
Privacy, safety, and security	Art. 28(1)	Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors on their service.
Assessing negative effects on the protection of minors	Art. 34(1)(d)	Providers of very large online platforms and of very large online search engines shall diligently identify, analyse, and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services. [...] This risk assessment shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, and shall include the following systemic risks: [...] (d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors, and serious negative consequences to the person's physical and mental well-being.
Mitigation measures to protect the rights of the child	Art. 35(1)(j)	Providers of very large online platforms and of very large online search engines shall put in place reasonable, proportionate, and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights. Such measures may include, where applicable: [...] (j) taking targeted measures to protect the rights of the child, including age verification and parental control tools, and tools aimed at helping minors signal abuse or obtain support, as appropriate.
Standardising targeted	Art. 44(1)(j)	The Commission shall consult the [European Data Protection] Board and shall support and promote the development and

mitigating measures		implementation of voluntary standards set by relevant European and international standardisation bodies, at least in respect of the following: [...] (j) standards for targeted measures to protect minors online.

These last few months, article 28 of the DSA has been at the forefront of the EU policy scene in the online child protection domain. In addition to forbidding targeted advertising aimed at minors (article 28(2)), it puts an obligation on providers of online platforms accessible to minors to 'put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service' (article 28(1)). To complement this rather vague wording, the European Commission published specific guidelines on 14 July 2025 (see the 'Age assurance under the DSA' section of this report for further details).

The AI Act

AI Act provisions dealing with minors in digital environments:

Concept	Article	Explanation
Prohibition of the exploitation of age-based vulnerabilities	5(1)(b)	The placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm is prohibited.
Specific attention to children in high-risk AI systems assessments	9(8)	When implementing the risk management system described in paragraphs 1 to 7, specific consideration shall be given to whether the high-risk AI system is likely to be accessed by or have an impact on children.

Besides these two articles, it is worth noting that Recital 48 of the AI Act underlines that 'children have specific rights as enshrined in Article 24 of the EU Charter [of Fundamental Rights] and in the United Nations Convention on the Rights of the Child (further elaborated in the UNCRC General Comment No. 25 as regards the digital environment), both of which require consideration of the children's vulnerabilities and provision of such protection and care as necessary for their well-being'.

Nonbinding measures

In addition to regulations and directives, some nonbinding texts, including guidelines, communications, recommendations, declarations, and statements by

bodies such as the Council of Europe, the European Commission, and the European Data Protection Board (EDPB) complement the existing EU-level framework of measures aimed at protecting minors and ensuring their rights online.

Nonbinding measures dealing with minors in digital environments at the EU level:

Item	Year	Explanation or title
Council of Europe Recommendation CM/Rec(2018)7	2018	Council of Europe Guidelines to respect, protect, and fulfil the rights of the child in the digital environment.
EDPB Guidelines 4/2019 on Article 25 - Data Protection by Design and by Default	2019	These EDPB guidelines specify that the principles of by default data protection and by design data protection, enshrined in art. 25 of the GDPR, must be adapted to children.
EDPB Guidelines 05/2020 on consent under Regulation 2016/679	2020	These EDPB guidelines specify that consent processes for personal data collection and processing under the GDPR must be adapted to minors.
Council of Europe Guidelines on Children's data protection in an education setting	2021	Council of Europe Guidelines on Children's data protection in an education setting.
European Commission Communication 2021/142	2021	EU Strategy on the Rights of the Child.
European Commission Communication 2022/212	2022	New European strategy for a better internet for kids (BIK+).
2023/C 23/01	2023	European Declaration on Digital Rights and Principles for the Digital Decade ('Protection and empowerment of children and young people in the digital environment' section).
European Commission Recommendation 2024/1238	2024	Recommendation on developing and strengthening integrated child protection systems in the best interests of the child.
European Commission Communication 2024/188	2024	Putting Children's Interests First: Communication accompanying the Commission Recommendation on Integrated Child Protection Systems.
EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR	2024	Art. 6(1)(f) of the GDPR states that when legitimate interest is used as a legal basis for processing the personal data of a minor, specific attention should be given to the balance between this legitimate interest and the minor's fundamental rights and freedoms. These EDPB guidelines add that this balancing exercise should

		ensure that the best interest of the child is the primary consideration, in accordance with the EU's Charter of Fundamental Rights and United Nation's Convention on the Rights of the Child.
Statement 1/2025 on Age Assurance	2025	EDPB Statement on Age Assurance.
2025/2060(INI)	2025	IMCO Committee Draft Report on the Protection of Minors Online, European Parliament
European Commission Communication C(2025) 4764 final	2025	European Commission Guidelines on article 28(1) of the DSA.

Appendix 2—Authorities responsible for enforcing GDPR, AVMSD, and DSA provisions mandating age assurance across the EU

Online platform	Provision that appears to be breached	Responsible authority or authorities
Discord	28(2) DSA	The *Autoriteit Consument en Markt* or ACM, the Dutch Authority for Consumers and Markets, is the main coordinating authority as the DSC of the country where Discord has established an entity in the EU.[42] In cooperation with *Autoriteit Persoonsgegevens,* the Dutch data protection authority (DPA), which shares responsibilities with the ACM under the DSA, particularly around personal data protection (profiling, transparency of recommender systems, etc.).
	6a(2) AVMSD	Discord is an instant messaging and VoIP[43] social platform that is not considered as a video-sharing platform service. It is therefore not covered by the AVMSD.
	6(1)(b) GDPR	The lead supervisory authority is *Autoriteit Persoonsgegevens,* the Dutch data protection authority, as the DPA of the country where Discord has established an entity in the EU. In addition, any DPA established in another EU Member State may act on enforcement, if relevant (e.g. if the breach particularly and specifically impacts its own citizens) and if the lead supervisory authority allows it.
	8 GDPR	
	National contract law	The civil courts, public authorities (e.g. consumer protection authorities), and/or specialised regulators of the country whose national contract law is being breached.
Fortnite	28(2) DSA	*Post- och telestyrelsen* or PT (Sweden's Post and Telecom Authority), is the main coordinating authority as the DSC of the country where Epic Games has appointed a legal representative in the EU in compliance with article 13 of the DSA. Integritetsskyddsmyndigheten (Sweden's Data Protection Authority), which shares responsibilities with the DSC under the DSA,

		particularly around personal data protection.
	6a(2) AVMSD	Fortnite is primarily an online multiplayer game, not an audiovisual media service. Although it includes elements that do involve audiovisual content, these are ancillary to the main purpose of the platform, which is gaming. Fortnite is thus not covered by the AVMSD.
	6(1)(b) GDPR	The lead supervisory authority is the *Commission nationale pour la protection des données* or CNPD, Luxemburg's data protection authority, as the DPA of the country where Epic Games, Fortnite's parent company, is established in the EU.[44] In addition, any DPA established in another EU Member State may act on enforcement, if relevant (e.g. if the breach particularly and specifically impacts its own citizens) and if the lead supervisory authority allows it.
	8 GDPR	
	National contract law	The civil courts, public authorities (e.g. consumer protection authorities), and/or specialised regulators of the country whose national contract law is being breached.
Instagram	28(2) DSA	European Commission
	6a(2) AVMSD	*Coimisiún na Meán* (Ireland's media regulator), as the media regulator of the country where Meta, Instagram's parent company, is established in the EU.[45] In cooperation with the Irish Data Protection Commission or DPC, since the matter overlaps with data protection.
	6(1)(b) GDPR	The lead supervisory authority is the Data Protection Commission or DPC, Ireland's data protection authority, as the DPA of the country where Meta, Instagram's parent company, is established in the EU. In addition, any DPA established in another EU Member State may act on enforcement, if relevant (e.g. if the breach particularly and specifically impacts its own citizens) and if the lead supervisory authority allows it.
	8 GDPR	
	National contract law	The civil courts, public authorities (e.g. consumer protection authorities), and/or specialised regulators of the country whose national contract law is being breached.
Roblox	28(2) DSA	*Autoriteit Consument en Markt* or ACM (Dutch Authority for Consumers and Markets), is the main coordinating authority as the DSC of the country where Roblox has appointed a legal representative, in compliance with article 13 of the DSA. *Autoriteit Persoonsgegevens* (Dutch Data Protection Authority), which shares responsibilities with the ACM under the DSA, particularly around personal data protection (profiling, transparency of recommender systems, etc.).
	6a(2) AVMSD	As an interactive gameplay and game creation platform, Roblox is not recognised as a video-sharing platform service. It is thus not covered by the AVMSD.
	6(1)(b)	The lead authority is *the Landesbeauftragten für den Datenschutz*

42 Unlike Fortnite (Epic Games) or Roblox, Discord does not specify in its Privacy Policy whether it has appointed a legal representative in the EU to comply with article 13 of the DSA or not. The only trace of a legal entity linked to Discord in the EU that can be found is that of Discord Netherlands B.V.

43 Voice over internet protocol (VoIP), also known as IP telephony, is a set of technologies used primarily for voice communication sessions over internet protocol (IP) networks, such as the Internet.

	GDPR	*und die Informationsfreiheit Baden-Württemberg* (the state DPA of Baden-Württemberg), as the DPA of the State were Roblox is established in Germany.[46] In addition, any DPA established in another EU Member State may act on enforcement, if relevant (e.g. if the breach particularly and specifically impacts its own citizens) and if the lead supervisory authority allows it.
	8 GDPR	
	National contract law	The civil courts, public authorities (e.g. consumer protection authorities), and/or specialised regulators of the country whose national contract law is being breached.
Snapchat	28(2) DSA	European Commission
	6a(2) AVMSD	*Coimisiún na Meán* (Ireland's media regulator), as the media regulator of the country where Snap, Snapchat's parent company, is established in the EU.[47] In cooperation with the Irish Data Protection Commission or DPC, since the matter overlaps with data protection.
	6(1)(b) GDPR	The lead supervisory authority is the Data Protection Commission or DPC, Ireland's data protection authority, as the DPA of the country where Snap, Snapchat's parent company, is established in the EU. In addition, any DPA established in another EU Member State may act on enforcement, if relevant (e.g. if the breach particularly and specifically impacts its own citizens) and if the lead supervisory authority allows it.
	8 GDPR	
	National contract law	The competition/markets authority of each EU Member State
TikTok	28(2) DSA	European Commission
	6a(2) AVMSD	*Coimisiún na Meán* (Ireland's media regulator), as the media regulator of the country where TikTok is established in the EU.[48] In cooperation with the Irish Data Protection Commission or DPC, since the matter overlaps with data protection.
	6(1)(b) GDPR	The lead supervisory authority is the Data Protection Commission or DPC, Ireland's data protection authority, as the DPA of the country where TikTok is established in the EU. In addition, any DPA established in another EU Member State may act on enforcement, if relevant (e.g. if the breach particularly and specifically impacts its own citizens) and if the lead supervisory authority allows it.
	8 GDPR	
	National contract law	The civil courts, public authorities (e.g. consumer protection authorities), and/or specialised regulators of the country whose national contract law is being breached.
Twitch	28(2) DSA	The *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (BfDI), the German Federal Commissioner for Data Protection and Freedom of Information, as the DPA of the country where Twitch has designated a legal representative in compliance with article 13 of the DSA.[49]

44 Through Epic Games International S.à.r.l.
45 Through Meta Platforms Ireland Ltd., in Dublin.

	6a(2) AVMSD	The *Autorité Luxembourgeoise Indépendante de l'Audiovisuel* or ALIA (Luxemburg's media regulator), as the media regulator of the country where Twitch is established in the EU.[50] In collaboration with the *Commission nationale pour la protection des données* or CNPD, Luxemburg's data protection authority, since the matter overlaps with data protection.
	6(1)(b) GDPR	The lead supervisory authority is the *Commission nationale pour la protection des données* or CNPD, Luxemburg's data protection authority, as the DPA of the country where Twitch is established in the EU. In addition, any DPA established in another EU Member State may act on enforcement, if relevant (e.g. if the breach particularly and specifically impacts its own citizens) and if the lead supervisory authority allows it.
	8 GDPR	
	National contract law	The civil courts, public authorities (e.g. consumer protection authorities), and/or specialised regulators of the country whose national contract law is being breached.
YouTube	28(2) DSA	European Commission
	6a(2) AVMSD	*Coimisiún na Meán* (Ireland's media regulator), as the media regulator of the country where Google, YouTube's parent company, is established in the EU.[51] In cooperation with the Irish Data Protection Commission or DPC, since the matter overlaps with data protection.
	6(1)(b) GDPR	The lead supervisory authority is the Data Protection Commission or DPC, Ireland's data protection authority, as the DPA of the country where Google, YouTube's parent company, is established in the EU. In addition, any DPA established in another EU Member State may act on enforcement, if relevant (e.g. if the breach particularly and specifically impacts its own citizens) and if the lead supervisory authority allows it.
	8 GDPR	
	National contract law	The civil courts, public authorities (e.g. consumer protection authorities), and/or specialised regulators of the country whose national contract law is being breached.

Acknowledgements

I would like to warmly thank the experts who were interviewed in the framework of this research, as well as those who kindly agreed to review drafts and provide feedback. Their input greatly contributed to informing and improving this paper. The views expressed here, however, do not necessarily reflect their own or those of their employers.

46 Through Roblox GmbH, in Stuttgart.
47 Through Snap Ireland Ltd., in Dublin.
48 Through TikTok Technology Ltd., in Dublin.
49 While the DSC has a general coordination role under the DSA, when it comes to article 28(2), the BfDI is the only competent authority. This may be the case in other EU Member States.
50 Through Twitch Interactive Luxembourg S.à.r.l.
51 Through Google Ireland Ltd., in Dublin.

Special thanks to:

- **Manon BAERT,** Senior EU Affairs Officer, 5Rights
- **Lena-Maria BÖSWALD,** Senior Policy Researcher, Digital Public Sphere, *interface*
- **Julie DAWSON,** Chief Policy and Regulatory Officer, Yoti
- **Simeon DE WOUTER,** Policy Advisor, European Digital Rights (EDRi)
- **Martin DRECHSLER,** Managing Director, Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM)
- **Julian JAURSCH,** Policy Advisor, German Digital Services Coordinator
- **Sven HERPIG,** Lead, Cybersecurity Policy and Resilience, *interface*
- **Michèle LEDGER,** Associate professor of Law, University Namur; Research Fellow, Centre on Regulation in Europe (CERRE)
- **Annabelle RICHARD,** Partner in the Technology Media & Telecommunications (TMT) Practice, Pinsent Masons France
- **Corbinian RUCKERBAUER,** Senior Policy Researcher, Digital Rights, Surveillance and Democracy, *interface*
- **Luisa SEELING,** Lead Writing, Editing & Publishing, *interface*
- **Davy WANG,** Lawyer and Case Coordinator, Gesellschaft für Freiheitsrechte (GFF)

Author

Jessica Galissaire
Senior Policy Researcher Digital Public Sphere
jgalissaire@interface-eu.org

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org
T +49 (0) 30 81 45 03 78 80
F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
Ebertstraße 2
D-10117 Berlin

Design by Make Studio
www.make.studio
Code by Convoy
www.convoyinteractive.com