



Council of the European Union
General Secretariat

Brussels, 10 November 2025

WK 12686/2025 INIT

LIMITE

**AUDIO
JEUN
CULT
SOC
SAN**

**DIGIT
RECH
CONSUM
TELECOM
CYBER
JAI**

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

CONTRIBUTION

From:	General Secretariat of the Council
To:	Audiovisual and Media Working Party
N° prev. doc.:	12798/25
Subject:	Protection of minors online, the Audiovisual Media Services Directive (AVMSD) and age verification - Comments from FI, ES, HR, IT, SK and DE

Delegations will find attached comments on the subject mentioned above (doc.12798/25) from the following delegations: Finland, Spain, Croatia, Italy, Slovakia and Germany.

WK 12686/2025 INIT

LIMITE

EN



FI COMMENTS

Discussion Protection of Minors on video-sharing platforms and online. Answers of the Finnish Delegation

24.9.2025

- 1. To what extent have the AVMSD provisions on protection of minors on video-sharing platforms been implemented in your Member State? Which of the prescribed measures do you see as the most effective and do you see any major obstacles or gaps, including in their implementation?**

To our knowledge, there are no VSP's established in Finland and therefore we do not have any concrete experience on the application of minor protection rules in this regard.

- 2. Do you see a specific need to strengthen the current provision on age verification in the AVMSD? For instance, to require a broader uptake, to refer to the interplay with other rules, to provide more harmonisation or to specify when such measures are to be considered appropriate?**

Finland supports the enhancement of the protection of minors in the digital environment. However, we believe that this should primarily be accomplished through general regulation, rather than by intervening in a single specific sector. It is also important to take into account other existing recent legislation concerning the protection of minors and to assess the adequacy of current regulation before initiating new legislative measures. For example, the practical experiences with the application of Article 28 of the DSA are still very recent, especially considering that the Commission's guidelines clarifying the application of the article were only published in the summer of 2025.

In the field of consumer protection, the objective should be to establish horizontal and sufficiently general regulation, ensuring that the rules are applicable to emerging phenomena in the digital environment and do not require continual revision. We also consider it important to ensure that any potential solutions for age verification do not weaken the protection of personal data or unnecessarily increase, for example, the processing of minors' personal data. To our understanding, one of the key challenges in the context of protection of minors is the lack of available age verification solutions within the EU. Therefore, before considering additional regulatory measures, efforts should be directed towards the development of reliable and privacy-preserving age verification solutions.

The potential age verification systems should also be developed keeping in mind the United Nations Convention on the Rights of the Child article 12, so that children's right to self-determination will not be endangered by providing control tools only to parents or guardians in the family.

Typically, technical tools will be circumvented quickly. VPNs, proxies, TOR, private browsers, disposable accounts, browser tricks and simple workarounds often let tech-savvy or determined minors reach blocked content.

One of the greatest risks related to increased protective and restrictive technologies could be the increased use of the TOR, which would increase the exposure to harmful content.

3. Which other tools and measures do you see as the most important to strengthen the protection of minors online?

We see that many of the challenges affecting minors can likely be addressed within the framework of effective enforcement of the existing regulatory instruments. The guidelines issued by the European Commission on the application of Article 28 of the Digital Services Act provide a valuable starting point in this regard, and it is essential to ensure that platforms comply with them as broadly as possible.

In addition, raising public awareness plays an important role in ensuring that citizens are informed about the potential harms posed by online platforms—both to themselves and to society at large—and are empowered to identify and respond to harmful or unlawful content. Media literacy will continue to play a central role in this regard, as minors must also be equipped with the necessary skills to protect themselves online.

Media literacy is needed to avoid the pitfalls and weaknesses of technical tools created for protection of minors. Over-blocking content based on cultural differences (for example nudity without sexual context, LGBTQ+ related content or suicide prevention information) could also restrict access to supportive and educative content online.

By enhancing critical thinking we can encourage minors to make justified choices in the online environment. Respecting children's autonomy would strengthen their dignity, promote their development, and support their ability to become responsible and engaged members of society.

BIK+ recognises minors as rights-holders who need skills, agency, safer environments, and support networks. This approach is more sustainable because it strengthens children's resilience instead of just restricting access.



ES COMMENTS

Audiovisual and Media Working Party

24 September 2025

Protection of minors online, the Audiovisual Media Services Directive (AVMSD) and age verification

1. *To what extent have the AVMSD provisions on protection of minors on video-sharing platforms been implemented in your Member State? Which of the prescribed measures do you see as the most effective and do you see any major obstacles or gaps, including in their implementation?*

Spain firmly believes that protecting minors from harmful content is an intergenerational responsibility that demands firm national commitment and collective European action. Protection of minors online is, in fact, **one of our current political and legislative priorities**.

Since the entry into force, in 2022, of the General Law on Audiovisual Communication, which transposes the 2018 Audiovisual Media Services Directive, all the measures prescribed in article 28b are mandatory for the video-sharing platforms under Spanish jurisdiction.

In addition to this, in the past few years we have engaged in a thorough and comprehensive process aimed at achieving the highest standards of protection of minors online. The cornerstone of our efforts is the **draft Organic Law for the Protection of Minors in Digital Environments**. This landmark legislation, approved by the Government in March 2025 and now in parliamentary process, aims to reinforce the legal framework in order to impose stricter measures, among others, on video-sharing platforms. In particular, once this draft organic law is passed:

- Minor protection **obligations will be extended** to video-sharing platforms **providers established outside the EU** if their services target the Spanish market.
- Video-sharing platforms and their users of special relevance will be required to include a link for easily filing **complaints with the national regulatory authority**.
- The obligation to establish and operate **age verification systems** to prevent minors from accessing harmful content will be reinforced, since:
 - These systems will have to comply with strict security, privacy, data protection, and data minimization requirements.
 - The regulatory authority will be granted powers to order the blocking of video-sharing platforms that fail to implement the required age verification systems.
 - Sanctions for the failure to establish and operate age verification systems will be strengthened.



- Furthermore, **influencers and content creators will be required** to use the minors' protection mechanisms provided by video-sharing platforms and to adhere to the principle of truthful information if they provide news and current affairs programmes.

Among all these measures, Spain is especially focused in the development of age verification systems, that we consider the first step towards an effective implementation of all the other measures. Since July 2024, we have been working on **Spain's Beta Digital Wallet**, based on the EU Digital Identity Wallet specifications, which is now significantly advanced and is undergoing cybersecurity certification. Spain's implication in this area is also reflected in our **participation in the European Commission's pilot project to develop a "white label" age verification solution**, offering to play a mentoring role thanks to the experience gained with the Beta Digital Wallet.

2. *Do you see a specific need to strengthen the current provision on age verification in the AVMSD? For instance, to require a broader uptake, to refer to the interplay with other rules, to provide more harmonisation or to specify when such measures are to be considered appropriate?*

As for the need to strengthen the provision on age verification in the Directive, we believe it is important to conduct a process of reflection and analysis so as to evaluate the possibility of introducing more detailed requirements in order to advance towards a **higher level of harmonisation at the EU level**. As mentioned before, we consider age verification mechanisms as the cornerstone of the whole system of minors' protection and of course, for this measure to be effective, it would be essential that it operates evenly at all EU member states.

For instance, in Spain, in the draft Organic Law for the Protection of Minors in Digital Environments, we have included a new requirement to ensure security, privacy, data protection, and data minimization on age verification systems and we have granted powers to the regulatory authority to block, with judicial authorisation, video-sharing platforms that fail to implement these systems.

Besides, taking into account the interplay with the Digital Services Directive and the new guidelines on the protection of minors under DSA Article 28(1), it would be necessary to carefully **evaluate the complete coherence of the whole regulatory framework**.

In general, we would also like to point out that, in any process that regulates or affects minors, they must always be given a voice.



3. *Which other tools and measures do you see as the most important to strengthen the protection of minors online?*

Apart from age verification systems, Spain is convinced that a **holistic approach** and a comprehensive use of all the available tools and measures for the protection of minors is necessary. In particular:

- We firmly believe in the potential of **parental control systems** to enable parents to supervise their children's activity online, acting as an extra layer of protection in order to avoid their exposure to harmful content.
- We also consider **co-regulation and self-regulation** as important mechanisms in times when technology evolves fast and industry actors need flexible and practical means that also involve them more directly, fostering cooperation and participation of all relevant actors in the protection of minors. For instance, right now, Spain's Ministry of Digital Transformation is working with other public and private actors in the drafting of a Protocol for promoting self-regulation of influencer marketing.
- Finally, we would like to underline the relevance of **media literacy** for the protection of minors online, so as to equip children and teenagers with the knowledge, skills and critical thinking they need to navigate the digital world safely. We could say that, if age verification systems are the key to the implementation of all the other measures, media literacy is the strongest, deepest and most powerful and long-term strategy to ensure that our minors are ready to protect themselves from the many multifaceted and changing risks they face online. Particularly in this area we find it essential to join forces, implicating public actors as well as the industry and the third sector.

Croatian written replies to Presidency background note on protection of minors online, the AVMS Directive and age verification (doc. 12798/25)

We would like to thank the Presidency for this useful initiative and hereby submit the following written replies to the guiding questions:

1. To what extent have the AVMSD provisions on protection of minors on video-sharing platforms been implemented in your Member State? Which of the prescribed measures do you see as the most effective and do you see any major obstacles or gaps, including in their implementation?

The Republic of Croatia has incorporated, through the Electronic Media Act, the provisions on the protection of minors on video-sharing platforms, in line with the AVMSD. We underline that there are currently no such platforms operating in Croatia, but we remain committed to the continuous work on the protection of minors. In addition to the legislative provisions, the regulatory authority adopted the **Rulebook on the Protection of Minors**¹, which further strengthened the obligations of stakeholders, as well as recommendations for the protection of minors in electronic media. The protection of minors does not cover programme content as such (series, films, etc.) nor advertising.

We would also underline that, for the past eight years, the Agency for Electronic Media, in cooperation with UNICEF and under the auspices of the Ministry of Culture and Media and the Ministry of Science and Education, has been organising the **Media Literacy Days**². Each year the event has a main theme; this year the focus was on raising awareness among children and young people about the digital footprint created by their online posts and the importance of privacy protection, as well as on education about disinformation and fact-checking. The event attracts a growing number of participants: this year more than 37,000 people – mostly children, young people and educators – took part; over 730 events and 2,100 activities were held in 191 towns and municipalities across Croatia; 1,220 preschool teachers, schoolteachers, librarians and professional associates organised activities and events, involving almost 400 primary and secondary schools and 65 kindergartens. Educational materials are published on the **Media Literacy website**³ and are freely available to all interested parties.

In addition to this initiative, the Croatian Regulatory Authority for Network Industries (HAKOM), which is also the national coordinator for the implementation of the DSA, marks the **Safer Internet Day**⁴ every February in cooperation with operators and other stakeholders. Updated brochures with key advice on safe internet use are sent to all fifth-grade pupils in Croatia and are intended for both children and parents. Through the child protection on the internet project, HAKOM experts carry out educational programmes for parents and pupils, providing them with information on responsible behaviour on social networks, especially when children begin to use the internet independently.

¹ [Pravilnik o zaštiti maloljetnika u elektroničkim medijima](#)

² [The 8th Media Literacy Days](#)

³ [Medijska pismenost -](#)

⁴ [Once again, HAKOM celebrates Safer Internet Day](#)

2. Do you see a specific need to strengthen the current provision on age verification in the AVMSD? For instance, to require a broader uptake, to refer to the interplay with other rules, to provide more harmonisation or to specify when such measures are to be considered appropriate?

We do not consider that more precise definitions or cross-references to other rules would necessarily result in stronger protection of minors. In our view, the most effective approach lies in direct engagement with children and in raising awareness among parents, educators, teachers and children themselves about potentially harmful content. We also believe that further harmonisation is not required, given the cultural differences and varying levels of media literacy across Member States.

3. Which other tools and measures do you see as the most important to strengthen the protection of minors online?

We consider systematic work on developing media literacy skills, especially **critical media literacy**, to be the most important tool. Critical media literacy facilitates the assessment of the credibility of information sources, recognition of disinformation and propaganda, and the distinction between advertising and editorial content. It also enables the safe use of artificial intelligence and various digital platforms. In addition, it is important to ensure effective implementation of the EU legislative framework, to make sure that global online platforms are genuinely responsible for the rights and protection of minors, that they restrict access to potentially harmful content, and that they take all measures to protect children from hate speech and cyberbullying.

PROTECTION OF MINORS ONLINE – ITALY

- 1. To what extent have the provisions of the Audiovisual Media Services Directive (AVMSD) on the protection of minors on video-sharing platforms been implemented in your Member State? Which of the measures provided for do you consider most effective, and do you identify any significant obstacles or shortcomings, including in their implementation?**

The provisions of the *Audiovisual Media Services Directive* (AVMSD) have been transposed into the Italian legislation by the Legislative Decree No. 208 of 2021 *Testo unico dei servizi di media audiovisivi* (TUSMA) – as last amended and supplemented by Legislative Decree No. 50 of 2024 – containing the consolidated text for the provision of audiovisual media services in consideration of market developments.

The second chapter of TUSMA – *Provisions applicable to platform services for sharing video, audio or both* – includes Articles 41 and 42, which deal respectively with the criteria for subjection to Italian jurisdiction and the protective measures that platform service providers must adopt.

Article 42 requires platform service providers subject to Italian jurisdiction to adopt measures – not necessarily codes of conduct or self-regulation (the adoption of which the Italian Communications Regulatory Authority - AGCOM - is nevertheless responsible for promoting) – aimed at protecting minors from programmes, user-generated videos and audiovisual commercial communications that may harm their physical, mental or moral development.

More specifically, it stipulates that these entities must take appropriate measures to protect minors from programmes, user-generated videos and audiovisual commercial communications that may harm their physical, mental or moral development, in accordance with Articles 37 and 43. These entities are also required to comply with the requirements of Article 43 in relation to commercially promoted, sold or organised audiovisual commercial communications.

What matters is what is stated in Article 41 regarding subjection to Italian jurisdiction.

It establishes that the subjection of such entities to Italian jurisdiction depends on their establishment in the national territory (specifying that AGCOM draws up a list of such entities).

More specifically, Article 41 stipulates that platform service providers are subject to Italian jurisdiction if they are established in Italy, or if the company that controls them or a subsidiary company is established in Italy, or if they are part of a group and another company in that group is established in Italy. Furthermore, if the controlling company or the subsidiary or other companies in the group are established in different Member States, the video-sharing platform provider is considered to be established in Italy if the controlling company is established there, or if one of its subsidiaries is established there, or if one of the subsidiaries first started its activity in Italy, provided that it maintains an effective and stable connection with the Italian economy.

The provision, by associating subjection to Italian jurisdiction with the aforementioned obligations referred to in Article 42 and the establishment of platform service providers in the national territory, hinders the application of the legislation itself to those providers who, although operating in the national territory, are not established there.

2. Do you consider there is a specific need to strengthen the current provision on age verification in the Audiovisual Media Services Directive (AVMSD)? For example, to require wider adoption, to refer to interaction with other rules, to ensure greater harmonisation, or to specify when such measures should be considered appropriate?

Regarding age verification measures, the following regulatory framework can be outlined.

With reference to the AVMS Directive, as transposed by Legislative Decree No. 208 of 2021, Article 42, paragraph 7, letter f) of the legislative decree in question specifies that video-sharing platform providers are in any case required to set up systems to verify, in compliance with personal data protection legislation, the age of users of video-sharing platforms with regard to content that may be harmful to the physical, mental or moral development of minors.

In this respect, as already indicated in response to question 1, it should be emphasised once again that the legislation limits its scope to video-sharing platform providers established in the national territory, thereby excluding those that are not established there.

On the other hand, the Communications Regulatory Authority has approved (Resolution 96/25/CONS) the procedures that video sharing platforms and websites that make content available in Italy must use to verify the age of users (known as age assurance, or age verification), with the aim of ensuring effective protection of minors from the dangers of the web, in implementation of Law No. 159 of 13 November 2023 ('Caivano Decree').

This age verification system involves the intervention of certified independent third parties to provide proof of age, defining a process based on two logically separate steps: identification and authentication of the identified person for each session of use of the regulated service (e.g., the provision of pornographic content via a website or web platform).

In case of age verification systems based on the use of applications installed on the device, an APP is made available to the user for the generation and certification of 'proof of age' (e.g., digital identity wallet APP, or digital identity management APP, etc.), which can be used for any purpose requiring identification. The user can therefore identify themselves and provide proof of age to the website or platform visited directly using the app installed on their device.

This system ensures a level of security appropriate to the risk and compliance with the minimisation of personal data collected. The 'double anonymity' mechanism does not allow age verification providers to know for which service the proof of age is being issued. At the same time, the proof provided to the website or platform does not contain any user identification data.

At the same time, the Communications Regulatory Authority has been selected by the European Commission to join a select group of Digital Services Coordinators, as referred to in European Regulation No. 2022/2065 (the Digital Services Act), to participate in testing the new application for verifying the age of minors accessing online platforms that host pornographic content.

Indeed, by introducing the obligation for online platforms to respect the fundamental rights of online users, particularly those of minors, Article 28 of the DSA stipulates that online platforms must ensure that their services offer younger users a high level of privacy, safety and security.

For this purpose, the European Commission is working on an age verification application, intended to provide a temporary solution pending the entry into force of the EU Digital Identity Wallet, scheduled for the end of 2026, in accordance with Regulation (EU) 2024/1183.

The application, based on the same technology planned for the EU Digital ID, will enable online service providers to verify whether users are aged 18 or over without compromising their privacy, further strengthening the protection of minors online.

The aim of the project is to develop, by summer 2025, an EU-wide harmonised and privacy-friendly age verification solution, including an open-source white-label application.

Through this application, users can request digital certification of their age ('proof of age') from certified third parties (e.g. digital identity providers). Proof of age, which does not contain any information about the user's identity, will be stored exclusively on the device on which the application is installed. When the user accesses sites or platforms reserved for adults, these will send a request for age verification and, through the same application (e.g. by scanning the QR code displayed by the site or platform), the user will be able to send the 'proof of age' directly and anonymously.

Based on its expertise in child protection, and in its capacity as DSC, AGCOM was therefore called upon to contribute to the testing of the app, with the aim of rapidly adopting the technological solutions shared at European level.

At the end of the trial phase, the solution implementing the measures established by the Authority will be harmonised with the European Commission's age verification application and will be made available for use by online sites and platforms offering content reserved for adult users.

Finally, it should be emphasised that the Digital Services Act aims to make greater use of soft law instruments, i.e. self-regulation, in line with the principle that it is not effective to regulate a constantly evolving sector such as the digital sector through rigid rules.

Therefore, it remains up to each Member State to take action on the issue of child protection, in the hope that every national legislative effort will be a driving force for a "European society" that is more attentive to children's rights, including in the digital world.

On this issue, it is worth noting that the Ministry of Enterprise and Made in Italy is supporting work on a bipartisan parliamentary legislative initiative aimed at defining safe spaces within which minors can explore the internet, with a view to maintaining the right balance between protection and freedom in the digital world.

Specifically, the initiative stipulates that minors under the age of fifteen should be prohibited from accessing social media, video sharing platforms and adult content.

Member States, sharing the same objectives of protecting minors in a digital environment, should cooperate to adopt effective legislation on the indication of a specific age, thus providing a uniform framework throughout the Union.

The technical advances achieved so far in age verification should now be translated consistently by Member States into clear regulations that oblige digital and social media service providers to verify the age of users effectively and accurately in a non-invasive and non-discriminatory manner.

3. What other tools and measures do you consider most important for strengthening the protection of children online?

In addition to age verification tools, initiatives to promote digital literacy remain of fundamental importance.

In this respect, the Ministry of Enterprises and Made in Italy has an Interinstitutional Advisory Committee for Media and Digital Literacy, as referred to in the Ministerial Decree of 19 June 2024.

This Body – which replaces the previous Committee for the Application of the Media and Minors Self-Regulation Code, which was mainly aimed at protecting minors in radio and television programmes – has the primary objective of streamlining the process of studying and researching the issues of digital literacy and the protection of minors, and of strengthening the principle of collaboration between all the administrations and authorities involved in working on these matters.

In carrying out its duties, the committee also draws on the technical support of a panel of experts in the fields of broadcasting and social media to promote a culture of digital wellbeing for minors.

Within the interinstitutional advisory committee – which is divided into three working groups according to the topics to be addressed – one working group is specifically dedicated to monitoring research and promotion activities aimed at raising awareness of the impact that new digital technologies have on children and adolescents in the current historical and socio-political context.

Protection of minors in relation to the classification of films released in cinemas. The Italian film classification system

Legislative Decree No. 203 of 7 December 2017, implementing the provisions of Article 33 of Law No. 220 of 14 November 2016, reformed the subject of film review by laying down new provisions on the classification of cinematographic works with regard to organisational, procedural and sanctioning aspects, providing for the establishment of a Commission for the Classification of Cinematographic Works, which replaced the Commission for Cinematographic Review.

The classification of cinematographic works is intended to ensure a fair and balanced balance between the protection of minors and freedom of thought and artistic expression; it is also proportionate to the needs of child protection and the protection of minors, with particular regard to the sensitivity and personality development of each age group and respect for human dignity.

To this end, films can be classified according to their target audience as follows:

- a. films for all audiences;
- b. films not suitable for children under 6 years of age;
- b-bis. films not suitable for children under 10 years of age (recently approved)
- c. works prohibited to children under 14 years of age (unless accompanied by a parent or guardian and at least 12 years of age);
- d. works prohibited to children under 18 years of age (unless accompanied by a parent or guardian and at least 16 years of age).

Each age group (with the exception of “works for all”) is accompanied by a series of icons indicating the presence of one or more sensitive topics, in order to highlight the reasons for restricting viewing of the work to one or more specific age groups.

Sensitive content is considered to be scenes that, based on the categories and criteria specifically indicated, could be potentially harmful to minors. They fall into the following six categories: violence, sex, use of weapons, language and profanity, use of drugs or alcohol, discrimination and incitement to hatred.

The classification is a tool designed for dual use:

- a) to help parents assess which works are suitable for their children to view and
- b) to support producers/distributors in choosing the most appropriate age group for their work.

It should be borne in mind that classification:

- is general, so it cannot take into account all specific situations, experiences, characteristics, as well as the particular sensitivities of each child;
- provides information on the presence or absence of content that is potentially harmful to the personal and social development of each child, but cannot provide information on the actual ability of children to fully understand the content shown on the cinema screen.

Legislative Decree 203 of 2017 therefore introduces a principle of accountability for film operators, who are required to identify the correct classification of the work based on the age group of the target audience and submit it to the Film Classification Commission for verification.

The members of the Film Classification Commission are chosen from among:

- University professors of law, lawyers, magistrates assigned to the juvenile court, administrative magistrates, state lawyers and parliamentary advisers;
- Experts with particular expertise in the pedagogical and educational aspects of child protection, or sociologists with particular expertise in social communication and the behaviour of children and adolescents:
- University professors of psychology, psychiatry or pedagogy, pedagogues and professional educators;
- Experts designated by the most representative parents' associations.
- Experts with proven qualifications in the film industry, such as critics, scholars or authors;
- Experts designated by the most representative animal protection associations.

FOLLOW-UP TO AVMWP 24/9 – PROTECTION OF MINORS – INFORMATION FROM SLOVAKIA

1. To what extent have the AVMSD provisions on protection of minors on video-sharing platforms been implemented in your Member State? Which of the prescribed measures do you see as the most effective and do you see any major obstacles or gaps, including in their implementation?

The provisions of the AVMSD on the protection of minors have been fully transposed into national legislation since 2022. The transposition was done on a one-to-one basis, without going beyond the minimum requirements of the Directive. Enforcement competence lies with the Council for Media Services (CMS), which also acts as the Digital Services Coordinator (DSC) under the DSA.

At EU level, the only significant issue has been the inconsistent timing of transposition of AVMSD across Member States, which resulted in delays in the practical enforcement of Article 28b provisions. In our national context, there has so far been limited practical experience in applying the measures under this article, mainly due to the relatively small number of registered platforms. However, according to the Mavise database, this is common for territories that are not hubs for such services.

However, a recent major case involving a micro VSP illustrated the practical application of the rules. The platform hosted very problematic content (including pornography, hate speech and self-harm), failed to register, and did not implement appropriate measures under either the AVMSD or the DSA. The case required a combined application of both frameworks. Given the small size of the service, there was only limited leeway for applying the DSA, which highlighted the complementarity between the two regimes: the AVMSD provides a content-focused *lex specialis*, while the DSA offers a systemic oversight *lex generalis*.

The case, initiated through cross-border cooperation, led to an administrative procedure under both the AVMSD and the DSA, which is now in its final stage. Ultimately, it resulted in the voluntary shutdown of the service by the provider. Rather than exposing legislative gaps, this case demonstrated how the two frameworks complement each other, especially in smaller markets where most VSPs are of limited size and DSA provisions are less likely to apply extensively.

One gap we would, however, highlight is the need to assess the level playing field between VSPs and audiovisual media services under the existing rules in AVMSD, given increasing competition and convergence between these types of services. In particular, the rules on commercial communications merit attention.

Regarding the most effective measures, we share the Directive's intention to rely on a combination of measures, as there is no one-size-fits-all approach, even among VSPs themselves. But we believe that the impact and need of specific measures depend on the risk profile of the service—for example, there are different levels of risk associated with adult-content platforms compared to general-content VSPs.

Age assurance is currently a priority topic in regulatory discussions, as reflected in the latest DSA PoM Guidelines on Article 28. We consider this focus logical given the potential impact of age assurance in addressing minors' access to harmful content. Additionally, there is growing policy debate around defining a potential age of majority, driven by increasing evidence of the negative effects of harmful content on minors.

Finally, we believe that the previous and forthcoming ERGA and EBMS reports on the AVMSD can provide valuable insights into potential improvements to make the regime more enforceable. Building on this regulatory experience, the upcoming AVMSD review presents an ideal opportunity to assess the effectiveness of existing measures.

2. Do you see a specific need to strengthen the current provision on age verification in the AVMSD? For instance, to require a broader uptake, to refer to the interplay

with other rules, to provide more harmonisation or to specify when such measures are to be considered appropriate?

Based on our recent case experience, we consider the current AVMSD provisions on age verification sufficient to handle similar cases in practice. In some Member States, however, some legal questions have emerged regarding the mandatory nature of age verification measures under Article 28b.

In addition, applying the concepts of proportionality and appropriateness from the Directive can be challenging in less clear-cut cases, particularly for lower-risk VSPs. Therefore, we suggest clarifying the hierarchy of measures, following the logic of Article 6a, which already differentiates between levels of content harmfulness. This would mirror the European Commission's Guidelines on Article 28 and provide more legal certainty.

Given the age of the Directive, AVMSD currently refers only to "age verification" without mentioning "age estimation" as an alternative age assurance method, as recognised in the DSA Guidelines. Updating the text to clarify the distinction between these methods and their appropriate use cases would be beneficial.

We have also observed reluctance among VSPs to facilitate compliance by third-party services (e.g. vloggers) available on their platforms. These third-party services are required to comply with AVMSD rules but often lack control over the user interface and platform functionalities (e.g. displaying local content classification systems). A clarification of VSPs' role in enabling the compliance of other services on their platforms would therefore be welcome.

Additionally, we would like to highlight several points raised by ERGA in its recent work, in its submission to the call for evidence on the Article 28 Guidelines in 2025 and in the 2021 and 2022 reports focusing on VSPs. Additionally, there will be an EBMS report aimed at the evaluation of the AVMSD with concrete suggestions from the regulatory practice to be adopted end of 2025. ERGA has underlined the difficulties NRAs face in consistently applying the "essential functionality" criterion when defining a VSP, which can lead to classification challenges. It has also stressed the value of harmonised age verification standards, which would benefit platforms, users and regulators alike, and encouraged the Commission to build on effective national measures already implemented under the AVMSD. Furthermore, EBMS has proposed a risk-differentiated approach, following the logic that the most harmful content (such as pornographic or violent material) should only be accessible through the strictest age assurance tools, such as age verification. Finally, EBMS promotes a balanced use of both age estimation and age verification, complemented by accessible, interoperable parental control tools.

In this context, we believe it may also be relevant to reflect ongoing Commission work on technological solutions (e.g. EU Digital Wallet, Miniwallet) to address fragmentation in age verification approaches. When deploying such tools, it is essential to balance the protection of minors with the right to privacy by ensuring GDPR compliance and promoting privacy-preserving technologies such as zero-knowledge proofs (ZKPs). It should also be acknowledged that simple circumvention methods (e.g. VPNs) can undermine the effectiveness of even robust systems. Defining a set of minimum standards – covering privacy, data protection and reliability – could therefore enhance the consistency and credibility of age verification mechanisms across the EU.

Finally, a general clarification of the interplay between the AVMSD and the DSA would be valuable. This would further enhance complementarities between the two regimes and reduce legal uncertainty. In addition, greater harmonisation of regulatory approaches and standards across Member States (including at the level of AVMSD) would strengthen the effectiveness, consistency and predictability of the framework for both regulators and service providers.

3. Which other tools and measures do you see as the most important to strengthen the protection of minors online?

We believe that an effective system for the protection of minors relies on a combination of complementary measures. Media literacy and parental involvement should be further emphasised as essential elements. Empowering users in the online environment requires not only equipping them with the necessary skills but also ensuring that they can apply these skills effectively in practice. At the same time, it is equally important to strengthen the media literacy of content creators themselves, to promote responsibility and awareness on both sides of the digital and media ecosystem.

We also advocate for stronger cooperation between NRAs and other relevant authorities, such as DSCs and consumer protection bodies. In our recent case, the unique institutional setup in Slovakia—where the media regulator also acts as the DSC—enabled a coherent application of regulatory tools, which proved very effective.

In this regard, we highlight the added value of the ongoing coordinated action between EBDS/EBMS and media regulators on pornographic platforms, led by WG6 of EBDS. This coordinated action focuses on addressing systemic risks related to minors' access to pornographic content and ensuring a consistent regulatory response across Member States. It enables closer alignment between the enforcement tools of media regulators under the AVMSD and the systemic obligations under the DSA. Through regular exchanges, joint assessments and coordinated case handling, this initiative strengthens the capacity of regulators to tackle cross-border cases more effectively, ensures greater legal clarity for platforms operating in multiple jurisdictions, and ultimately improves the protection of minors online.

COMMENTS FROM GERMANY

Written Reply by Germany regarding question on effective protection of minors in the digital Environment.

Effective protection of minors in the digital environment requires clear and enforceable safeguards. A central element in this context are appropriate systems of mandatory age verification. These systems should be designed in an age-appropriate and risk-based manner to reliably protect children and young people from harmful or unsuitable content and services. Platforms carry a particular responsibility in this regard: they should ensure that age limits are consistently enforced through appropriate technical and organizational measures. Germany welcomes the fact that the Commission has now developed guidelines for the protection of minors. We hope that the guidelines will simplify the enforcement of the Digital Services Act (DSA). However, the guidelines do not make age verification mandatory for all relevant online platforms, including social media. We therefore support appropriate mandatory age verification for social media access.

At the same time, age verification must be implemented in a data-minimizing way. Safeguarding privacy and complying with data protection standards are essential components of youth protection. Systems should therefore be designed to provide a high level of security without collecting or storing unnecessary personal data. Youth protection and data protection must be pursued in parallel and not at the expense of one another. Adding to this the cost of implementing and using the protection has to be feasible for the respective enterprises and should not endanger their business model. Administrative overhead needs to be reduced as far as possible.

The regulatory framework for youth protection is shaped by the interplay between the Audiovisual Media Services Directive (AVMSD), the Digital Services Act (DSA), and national legislation such as the German Interstate Treaty on the Protection of Human Dignity and Minors in Broadcasting and Telemedia (JMStV) and the Federal Protection of Young Persons Act (JuSchG). Coherence and legal clarity as well as complementing European and national law are required to ensure effective implementation.

An increasing challenge in terms of child and youth protection in the media is the advancing AI technology. Beside a mandatory age verification, it is therefore also necessary to assess and take into account the risks associated with AI. Chatbots, for instance, are getting more and more realistic. They can have endless chat conversations with children and, therefore, get them easily addicted. AI-based image creator software enable the users to produce deepfakes or deepnudes of other people. Deepfakes are therefore not only questionable in their fundamental nature, but also particularly dangerous with regard to sextortion and cyberbullying. Lastly, deepfakes are contributing to the dissemination of fake news.

In addition to technical safeguards, self-regulation mechanisms and educational measures play an important role. Promoting media literacy, critical thinking, and awareness of digital risks strengthens the ability of young users to navigate online environments responsibly. Complementary tools such as parental controls and transparent content rating contribute to address different age groups and risk levels and to balance protection and self-determined media use.

Finally, cooperation and technical collaboration, also with media authorities, are crucial. Joint solutions, transparent default settings, effective reporting and redress mechanisms, clear requirements for recommendation algorithms, and supportive parental tools can all contribute to a more robust system of youth protection. Good interaction between operating systems of devices and age rating or youth protection systems can be an additional important technical element for effective youth media protection.

Taken together, effective youth protection depends on the combination of reliable age verification, privacy-compliant implementation, coherent regulation and supervision, educational support, and innovative technical measures.