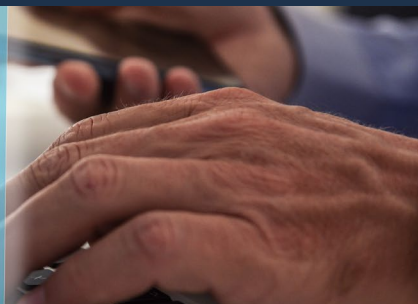
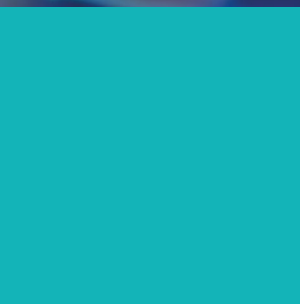




AVMSDigest

SAFE SCREENS: PROTECTING MINORS ONLINE



AVMSDigest

Safe Screens: Protecting minors online

European Audiovisual Observatory, Strasbourg, 2024

Director of publication Susanne Nikoltchev, Executive Director

Editorial supervision Maja Cappello, Head of Department for Legal Information

Editorial team Amélie Lacourt, Eric Munch, Justine Radel-Cormann, Sophie Valais

Authors (in alphabetical order) Amélie Lacourt, Eric Munch, Justine Radel-Cormann

Contributing authors Laura Ene

Editorial assistant Sabine Bouajaja

Research assistant Mario Gheza

Proofreading Linda Byrne

Cover layout Big Family

Layout Big Family

Obsy illustrations Philippe Lacourt

Press and Public Relations Alison Hindhaugh, alison.hindhaugh@coe.int

Publisher

European Audiovisual Observatory
76 Allée de la Robertsau – 67000 Strasbourg – France
Tel.: +33 (0)3 90 21 60 00 • Fax: +33 (0)3 90 21 60 19
iris.obs@coe.int • www.obs.coe.int

Please quote this publication as:

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

This publication, prepared by the European Audiovisual Observatory is based on information extracted from the projects [“The protection of minors on VSPs: age verification and parental control”](#) and the [AVMSDatabase](#), which have been carried out with the support of the MEDIA strand of Creative Europe.

The analyses presented in this report cannot in any way be considered as representing the point of view of the members of the European Audiovisual Observatory, the Council of Europe or the European Commission.

© European Audiovisual Observatory (Council of Europe), Strasbourg, 2024

AVMSDigest

SAFE SCREENS: PROTECTING MINORS ONLINE

Amélie Lacourt, Eric Munch, Justine Radel-Cormann

A PUBLICATION
OF THE EUROPEAN AUDIOVISUAL OBSERVATORY



O

TABLE OF CONTENTS

1	INTRODUCTION	
1.1	Foreword	7
1.2	What are video-sharing platforms	8
1.3	Legislation snapshot	10
1.4	State of the art	11
<hr/>		
2	HARMFUL CONTENT ON VSPS	
2.1	Defining what is harmful	13
2.2	What is harmful in practice?	15
<hr/>		
3	MEASURES PROTECTING MINORS AT NATIONAL LEVEL	
3.1	Article 28b (3) AVMSD	17
3.2	Reporting/flagging (Article 28b(3)(d) AVMSD)	19
3.3	Age verification (Article 28b(3)(f) AVMSD)	22
3.3.1	Age verification	22
3.3.2	Minimum age for VSP access	25
3.4	Parental control (Article 28b(3)(h) AVMSD)	26
3.5	Protection of minors' data (Article 28b(3), final § AVMSD)	29
<hr/>		
4	ENFORCEMENT	
4.1	Assessment of measures	33
4.2	Status of VPS registration in the MAVISE database	34
4.3	How NRAs assess the measures put in place by VSPs	35
4.4	Request for adaptation	36
4.5	Sanctions	37
<hr/>		
5	VSPS' MEASURES IN PRACTICE	
5.1	Introducing the measures	41
5.2	Account creation: step 1 - age verification	44
5.3	Account creation: step 2 - default settings	45
5.4	Using the service: ensuring minors see appropriate content only	46
5.5	Additional layer of protection with parental control	48
5.6	Reporting and flagging content	50
<hr/>		
	FURTHER INFORMATION	51

1

INTRODUCTION

1.1 Foreword

Providing readers with comprehensive information about national legislation has long been one of the European Audiovisual Observatory (EAO)'s missions. Readers familiar with our reports know that extensively mapping the rules across Europe is key to producing useful and trustworthy reports – although this means they are sometimes difficult to comprehend for the less experts of our readers.

As with the first issue of the AVMSDigest on the promotion of European works, this publication seeks to bridge the gap between a detailed overview of rules and a more accessible format. It reflects the results of our research on the protection of minors on video-sharing platforms (VSPs) through a study of the national transpositions of Article 28b of the Audiovisual Media Services Directive (AVMSD) across Europe.

In the context of VSPs, reporting on the rules only would not allow the drawing of a full picture of the situation, hence the decision to also rely on the general terms and conditions of VSPs, information from the EAO's AVMSDatabase, MAVISE database and practical testing of the measures in place. It should also be borne in mind that, under the country-of-origin principle, the rules applicable are those of the country in which the service provider is established, not those of the country from which the service is accessed.

It has been particularly useful to go a bit beyond the purely legal outlook and into the territory of practical verifications, and provide information that will prove interesting and useful to all of our readers.

With the entry into force of an online safety code in Ireland, Article 28b AVMSD will have been fully transposed in all EU member states. But how have these rules been transposed, and how do they work in practice? These are some of the questions that this publication aims to answer, looking into the EU-27, EFTA and UK.

Enjoy the read!

Strasbourg, September 2024

Maja Cappello

*Head of the Department for Legal Information
European Audiovisual Observatory*

1.2 What are video-sharing platforms?

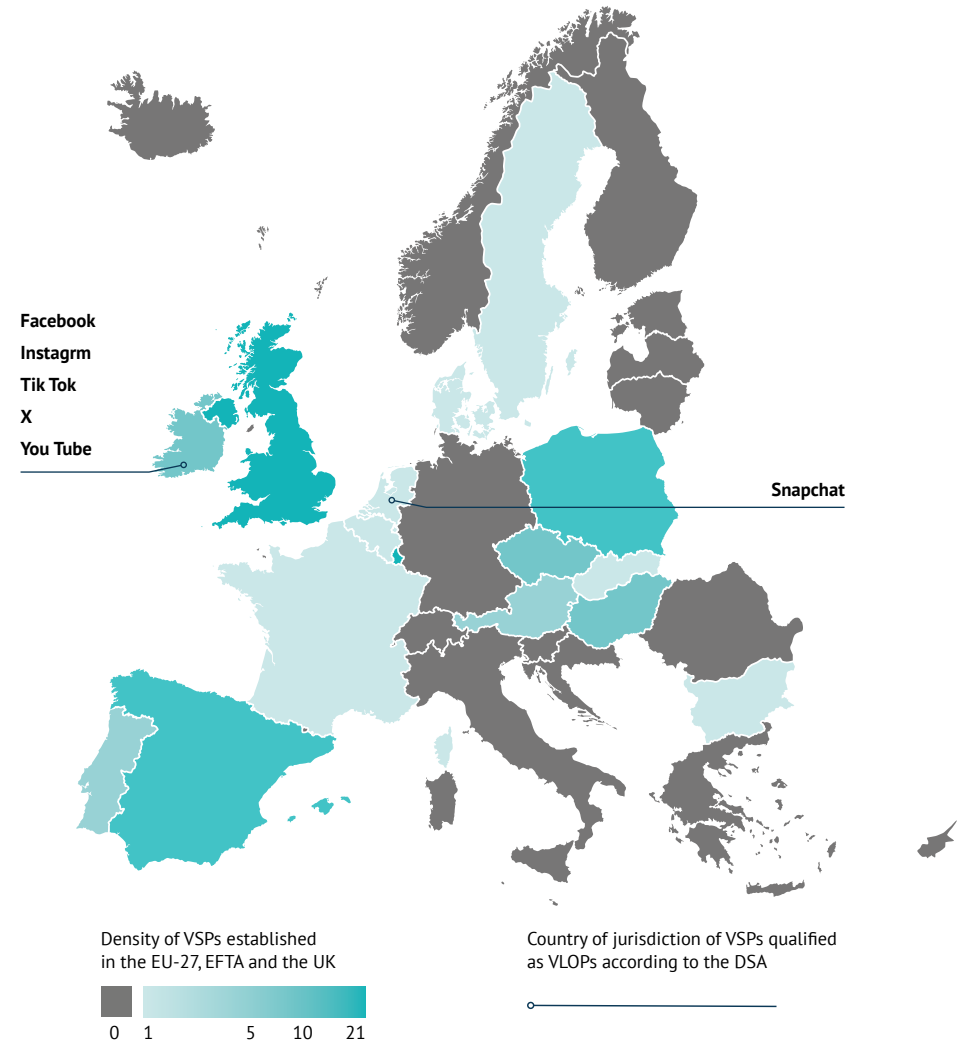
The AVMSD defines VSPs as follows:

“ **Article 1(1)(aa):** ‘video-sharing platform service’ means a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing. ”

At the moment of writing, according to the EAO’s MAVISE database, there were 107 VSP services¹ established in the EU-27, UK and EFTA countries (Norway, Iceland, Liechtenstein, and Switzerland). With the exception of adult VSPs which tend to target audiences beyond the borders of their country of jurisdiction, a majority of services mainly target the country in which they are established despite being accessible from abroad as well.

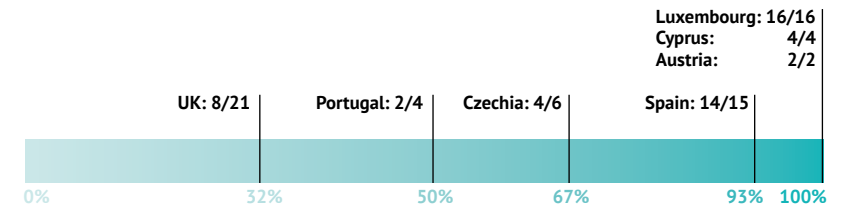
This publication looks at the measures put in place by six VSPs recently designated as VLOPs by the European Commission under the Digital Services Act (DSA)² (Facebook, Instagram, Snapchat, Tik Tok, X (formerly Twitter), and YouTube). These VSPs count more than 45 million users per month in the EU-27.

Fig 1. Number of VSPs established in the EU-27, EFTA and UK



Adult VSPs established in the EU-27, EFTA and UK

Based on the total number of VSPs established in each country



Source: EAO elaboration based on MAVISE search of VSPs established in the EU-27, UK and EFTA (3 September 2024)

1 Based on a search conducted on 3 September 2024

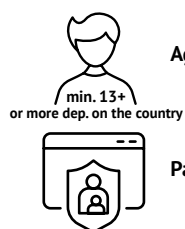
2 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065>

1.3 Legislation snapshot

Article 28b(1)(a) AVMSD read with Articles 28b(3)(a, d, f, g, h) AVMSD



Member states must ensure that VSPs set up measures to protect minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development.



Age verification measures



Content rating measures



User-friendly mechanisms to report and flag content



Parental control tools

Article 28b(5) AVMSD



Member states must establish the necessary mechanisms to allow national regulatory authorities (NRAs)/bodies to assess the appropriateness of the measures taken by VSPs under Article 28b (3).



VSPs comply with obligations



VSPs do not comply with obligations

- 1) Request for compliance
- 2) Possibility for sanctions in case of non-compliance

Regarding the six VSPs mentioned above, the Irish NRA is responsible for assessing the measures implemented by Facebook, Instagram, TikTok, X, and YouTube and the Dutch NRA for Snapchat.

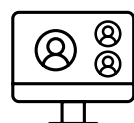
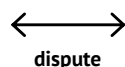
Article 28b(7) AVMSD



Member states must ensure that out-of-court redress mechanisms are available for the settlement of disputes between users and VSPs relating to the application of Art. 28b(1) and (3).



Disputes must be settled impartially and not deprive users of the legal protection afforded by national law.



Article 28a (1) (2) AVMSD and Article 3 E-commerce directive

Country-of-origin principle: a VSP must enforce the rules of the country in which it is established and not that of the country of any user located in the EU.

A VSP established in Ireland is subject to Irish rules



Irish rules apply instead of the targeted country's (exceptions exist)

CJEU case law:

Google Ireland, 9 November 2023: EU member states cannot impose general content moderation obligations on platforms established in other member states, upholding the country-of-origin principle. This decision came in response to Austria's attempt to apply its laws to Google, Meta, and TikTok, despite their being established in Ireland. The court emphasised that exceptions to this principle can only be applied on a case-by-case basis, not through general and abstract measures.



Detailed obligations are acceptable



General obligations are not acceptable

1.4 State of the art

The country-of-origin principle (Article 28a AVMSD) requires VSPs to comply with rules of their establishment country. Major VSPs are established in Ireland (Facebook, Instagram, TikTok, X, YouTube) or the Netherlands (Snapchat), but most EU countries have at least one VSP under their jurisdiction.

Article 28b AVMSD, aimed at protecting minors from harmful content, has been transposed across Europe, with varying approaches.

The AVMSD does not specifically define harmful content, leading to different interpretations. While most countries have literally transposed the Directive without additional guidance, some have provided further clarification on what constitutes harmful content, either by referring to violence or pornography or by providing further details, or by simply delegating the definition to other bodies.

Protection measures include age verification, parental control, and content rating, as provided for in the AVMSD. For example, age verification is clearly indicated in the national legislations of 20 EU member states, as well as Iceland and the UK, while parental control systems are referenced in the national legislations of 21 EU member states and Iceland, but not in the UK. The implementation of reporting and flagging mechanisms also appears clearly in the national legislations of most countries within the scope of this report, and so do rules regarding the use of minors' data, but this is not the case in all.

NRAs oversee compliance, assess protection measures, and sometimes handle out-of-court dispute resolutions between users and VSPs. There are also cases where out-of-court redress mechanisms are ensured through alternative mechanisms like arbitration/mediation systems or through internal VSP processes.

2

HARMFUL CONTENT ON VSPS



2.1 Defining what is harmful

Article 28b(1)(a)

AVMSD requires countries to ensure that VSPs protect minors from content that could harm their physical, mental, or moral development. This includes programmes, user-generated videos, and audiovisual commercial communications. The AVMSD allows flexibility for countries to define harmful content, enabling regulations adapted to cultural contexts but resulting in varied national implementations.



KEY FACTS

When transposing Article 28b(1)(a), countries have taken different approaches:

→ **References to violence or pornography:** 9 countries (BE (DE and VL), CY, FI, GR, HR, MT, PL, RO, and SK) have explicitly mentioned content that could impair minors' development, such as gratuitous violence and pornography, referring to Art. 6a(1) AVMSD.

→ **General reference to minors' development:** 15 countries (AT, BE (FR), CZ, DK, EE, ES, FR, HU, IS, LU, LV, PT, SE, SI and UK) have referred more generally to content that may impair minors' development without specifying particular types of content.

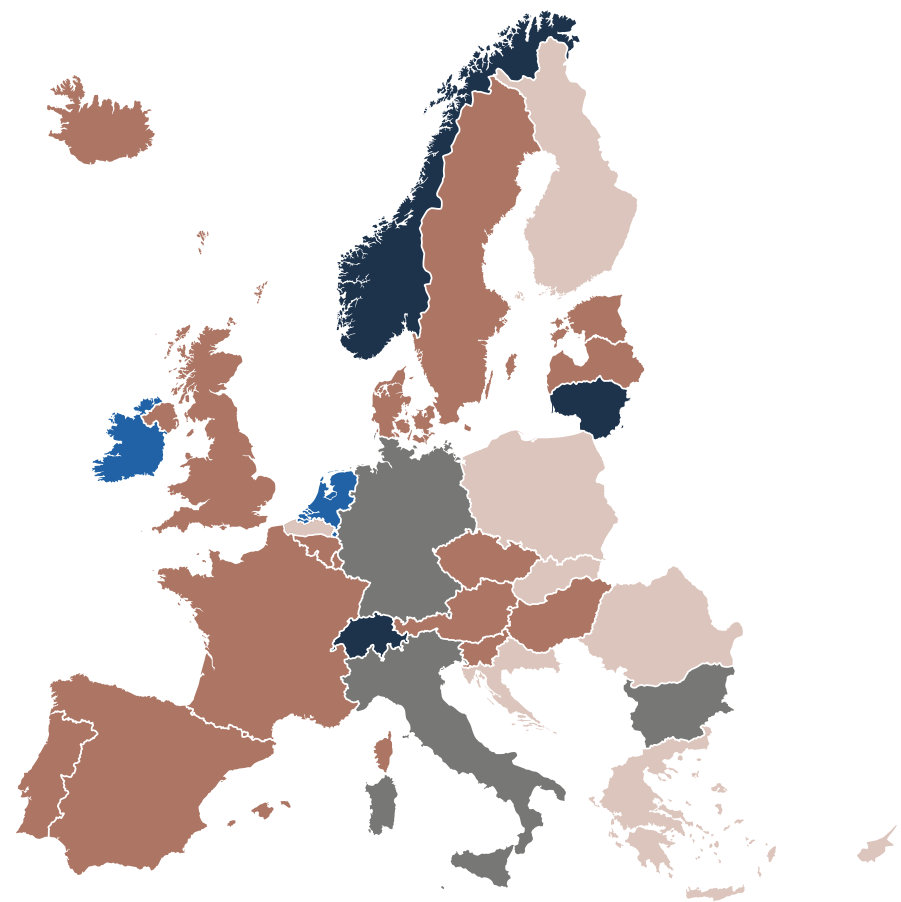
→ **Additional guidance through codes of conduct or specific legislation:** 3 countries (BG, DE, and IT,) have added more specific

guidance through codes of conduct or by providing detailed information in primary legislation.

→ **Delegated responsibility to other entities:** 2 countries (IE and NL) have delegated the responsibility to further define the rules for content regulation. In Ireland, *Coimisiún na Meán* is tasked with establishing an online safety code, while in the Netherlands, VSPs must develop their own codes of conduct.

→ **Other approaches:** 1 country (LT) refers to content that disseminates information detrimental to minors. 3 countries (CH, LI, and NO) aligned with Article 6a(1) of the 2010 Directive when they regulated audiovisual media services.

Fig 2. Approaches to national transpositions of Article 28b(1) AVMSD



- General reference to minors' development
- References to violence or pornography
- Additional guidance through codes of conduct or specific legislation

- Other approaches
- Delegated responsibility to other bodies

Source: European Audiovisual Observatory, AVMSDatabase and additional research (September 2024)

2.2 What is harmful in practice?

Zoom on detailed legislations (codes of conduct or specific legislation):

→ 3 countries (BG, DE, IT,) have added specific guidance through codes of conduct or by providing detailed information in primary legislation on what content may impair minors' physical, mental, or moral development.

Legislation with more details

GERMANY	ITALY
<p>Article 5a of the Interstate Treaty on the Protection of Minors in the Broadcasting and Telemédia requires VSPs to take appropriate measures to protect children and young people from content that could impair their development.</p> <p>Article 5 of the same law provides a more detailed definition, stating that content is considered potentially harmful to minors' development if it has not been approved for children or adolescents in the relevant age group according to the Protection of Minors Act. Paragraph 1 of this article specifies the age groups in the following way:</p> <ul style="list-style-type: none"> • 6 years or older, • 12 years or older, • 16 years or older, • 18 years or older. 	<p>The legislative Decree No 208 of 8 November 2021 specifies the types of content that may impair the physical, mental, or moral development of minors. It refers to Articles 37 and 38 (transposing Article 6a(1) AVMSD) on programmes that could seriously harm minors, including those containing:</p> <ul style="list-style-type: none"> • Gratuitous, insistent, or extreme violence, • Pornographic scenes, • Films that have been prohibited for public screening to children under 18 by competent authorities.

Code of conduct

BULGARIA
<p>The Radio and Television Act (Art. 19e(1)) mentions programmes which may impair the physical, mental, moral or social development of minors in accordance with the previously adopted Article 17a(1) to (3).</p> <ul style="list-style-type: none"> • The Council for Electronic Media together with the media service providers shall draw up a Code of Conduct containing measures for the assessment, indication and limitation of access to programmes which are harmful or pose a risk of impairing the physical, mental, moral or social development of minors.

3

MEASURES PROTECTING MINORS AT NATIONAL LEVEL



3.1 Article 28b (3) AVMSD

Article 28b(3) AVMSD introduces a series of measures that member states can impose on VSPs under their jurisdiction to ensure that users under the age of 18 are appropriately protected, as foreseen by Article 28b(1) AVMSD.

“ For the purposes of paragraphs 1 and 2, the **appropriate measures shall be determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake**, including those of the video-sharing platform providers and the users having created or uploaded the content as well as the general public interest.

Member States shall ensure that all video-sharing platform providers under their jurisdiction apply such measures. **Those measures shall be practicable and proportionate, taking into account the size of the video-sharing platform service and the nature of the service that is provided.** Those measures shall not lead to any ex-ante control measures or upload-filtering of content which do not comply with Article 15 of Directive 2000/31/EC. For the purposes of the protection of minors, provided for in point (a) of paragraph 1 of this Article, the most harmful content shall be subject to the strictest access control measures. [...] ”

This article establishes that the appropriateness of the measures taken is to be determined based on several factors and that those measures shall be practicable and proportionate, which implies that there is no “one size fits all” solution applicable to all VSPs. Parental control (Article 28b(3)(h) AVMSD), on the other hand, is not adapted to all VSPs. Adult VSPs explicitly prohibit minors from accessing their platforms, making the built-in parental controls of adult VSPs unnecessary.

A quick look at specific EU member states:

In the Netherlands and Latvia, the measures are not described in law, and the law instead imposes upon VSPs established in the country to have codes of conduct prescribing appropriate measures. Sweden and Finland³ do not describe the types of measures to be put in place by VSPs under their jurisdiction.

Key concepts

Article 28b(3) refers to several key concepts which are not defined in the AVMSD. Below are the most common defining elements of these concepts, based on the analysis of the measures developed by VSPs.

→ **Age verification** refers to any measure aimed at determining either the precise age of the user or if they are above a certain age limit. Basic measures include asking the user to provide their age, with no proof required, while more complex measures may imply providing official identification documents. Basic measures are generally less effective than the more complex ones, which in turn are generally more cumbersome for the user.

→ The notion of **parental control** regroups all types of measures and tools allowing parents or legal guardians to supervise a minor’s activity on VSPs. They include requiring validation from a parent upon signing up to a service and tools allowing an adult to oversee a minor’s activity on a VSP, by restricting access to certain contents or features (like direct messaging) or monitoring use history.

→ **Reporting and flagging mechanisms** allow users to bring to the attention of the VSP’s administrators content that they believe is infringing the terms and conditions of the platform, or to which access should be restricted to adults only. As such, reporting and flagging may result in the removal of the content or its categorisation.

3.2 Reporting/flagging (Article 28b(3)(d) AVMSD)

Among the measures mentioned by Article 28b(3)(d) AVMSD are reporting or flagging mechanisms:

“ (d) establishing and operating **transparent** and **user-friendly** mechanisms for users of a video-sharing platform to report or flag to the video-sharing platform provider concerned the content referred to in paragraph 1 provided on its platform ”

Most countries within the scope of this report have transposed Article 28b(3) AVMSD into their national legislation, but not all have provided the same level of detail on reporting and flagging mechanisms.



KEY FACTS

→ With the exception of **FR, LV, NL, and SE**, all EU member states have included in their national transpositions the obligation on VSP providers to provide transparent and user-friendly mechanisms to report or flag content.

→ **FR** refers to those mechanisms, but it does not refer to them being transparent and easy to use.

→ **The UK** only refers to users being able to “easily report” content.

→ **BE(VL)** is the only territory where the law explicitly links the reporting and flagging mechanism on VSPs to commercial communications only.

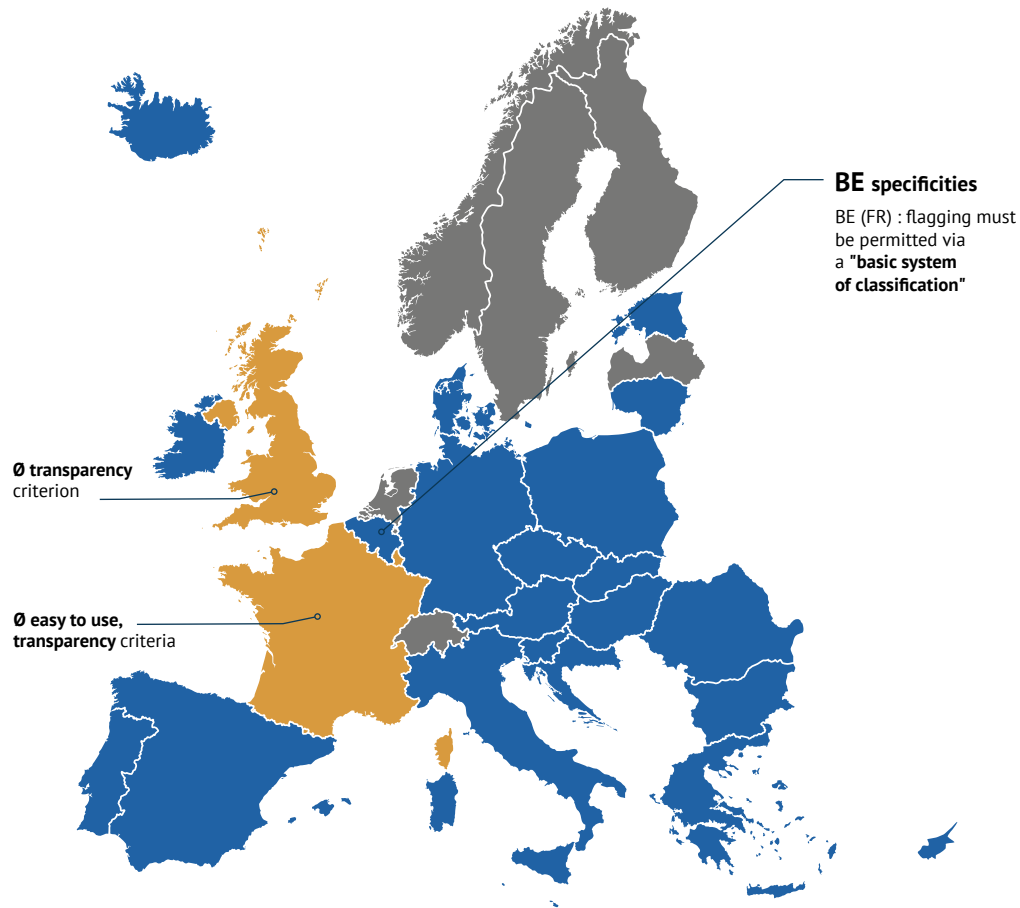
→ **BE(FR)** does not describe the mechanisms as easy to use.

→ **The majority of EU member states** (AT, BE(DE), BG, DE, HR, CY, CZ, DK, DE, ES, GR, HU, IE, IT, LT, LU, MT, PL, PT, RO, and SK) either transposed the dispositions of Article 28b(3)(d) verbatim or substantially literally.

→ **EFTA countries** (with the exception of IS) have not yet aligned their national legislation with the provisions of Article 28b (3) and make no mention of reporting and flagging mechanisms to protect minors on VSPs.

³ In Finland, the Act of Åland (2011: 95) on radio and television broadcasting describes the measures to be put in place by VSPs under the jurisdiction on Finland, but it only applies to the autonomous region of Åland.

Fig 3. National rules regarding reporting and flagging mechanisms



● National rules refer to a transparent and easy-to-use system

● No mention of reporting or flagging mechanisms

● National rules do not include all criteria listed under Article 28b(3)(d) AVMSD

Source: European Audiovisual Observatory, AVMSDatabase and additional research (September 2024)

Overview of national transpositions of AVMSD rules regarding reporting and flagging mechanisms:

Countries with verbatim and substantially literal transpositions of Article 28b(3)(d) AVMSD

AT, BE(DE), BE(VL), BG, DE, HR, CY, CZ, DK, EE, ES GR, HU, IE, IS, IT, LT, LU, MT, PL, PT, RO, SI, SK and UK

Countries with broader or more detailed transpositions of Article 28b(3)(d) AVMSD
VSP providers shall:

BE(FR)	Decree on audiovisual media services and video-sharing services February 2021 - Art. 2.5-2	<ul style="list-style-type: none"> • Make available to users uploading content a system for flagging such content according to a basic system of classification; • Make available to users a system for flagging content to the VSP provider according to a basic system of classification, and for informing users of the effect given to that flagging by the provider; • Ensure that such measures are transparent, user-friendly, easy-to-use and efficient.
FR	Law No. 86-1067 of 30 September 1986 on the freedom of communication (Loi Léotard) Consolidated 18 August 2022 - Art. 60 II	Make content classification and notification mechanisms available to users.



Some countries refer to reporting and flagging mechanisms without indicating that such mechanisms should be easy to use and transparent

3.3 Age verification (Article 28b(3)(f) AVMSD)

3.3.1 Age verification

Article 28b(3)(f) AVMSD introduces the obligation for VSPs to put in place age verification measures:

“ (f) establishing and operating age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors ”

As was the case with reporting and flagging mechanisms, there are differences in national transpositions of Article 28b(3)(f) AVMSD, with some of them reusing the wording of the AVMSD verbatim or rephrasing it but keeping the meaning.



KEY FACTS

→ Most EU member states (AT, BE, BG, HR, CY, CZ, DK, FR, DE, ES, GR, HU, IE, IT, LT, LU, MT, PT, RO, SK, SI) mention age verification as one of the measures to be implemented by VSP providers, if appropriate, in order to protect minors.

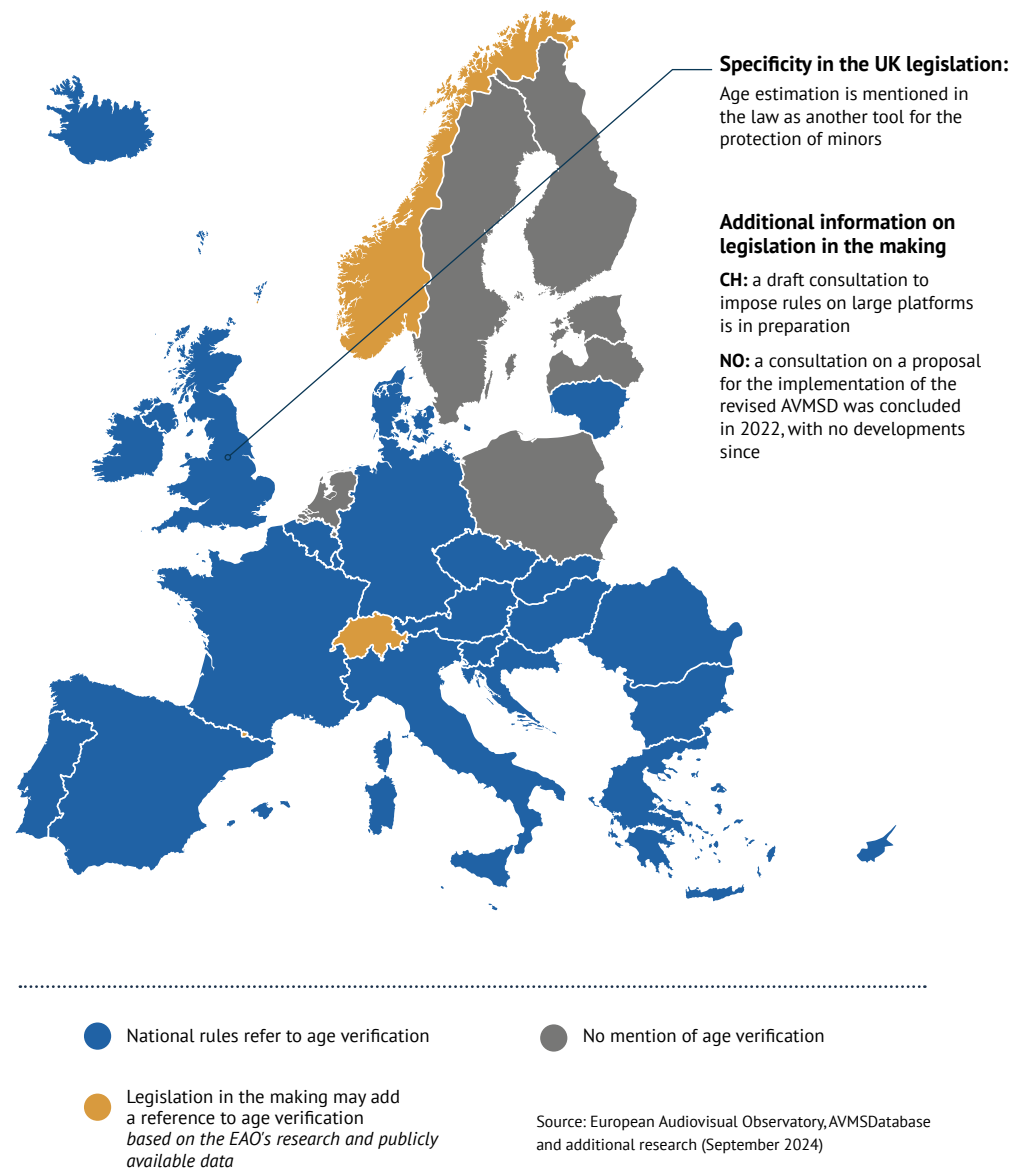
→ In PL, age verification is not mentioned, with the law only indicating the need for technical safeguards “including parental control systems or other appropriate means [...]”.

→ The UK is the only country in which the law references age estimation⁴ in addition to age verification.

→ National transpositions of the AVMSD include no reference to age verification in EE, FI, LV, NL and SE.

→ With the exception of IS, EFTA countries have not yet aligned their national legislations with the dispositions of Article 28b (3) and make no mention of age verification to protect minors on VSPs.

Fig 4. National rules regarding age verification (Article 28b(3)(f) AVMSD)



⁴ Age estimation relies on algorithms estimating the age of a user based on a facial analysis of a picture taken upon signing up or logging in to an online service.

Overview of national transpositions of AVMSD rules regarding age verification:

Countries with verbatim and substantially literal transpositions of Article 28b(3)(f) AVMSD

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.
UK	Online Safety Act 2023 Section 12(3)(a), (4)	A service using proportionate systems and processes designed to prevent children of any age from encountering, by means of the service, primary priority content that is harmful to children; This duty requires a provider to use age verification or age estimation (or both) to prevent children of any age from encountering primary priority content that is harmful to children which the provider identifies on the service.

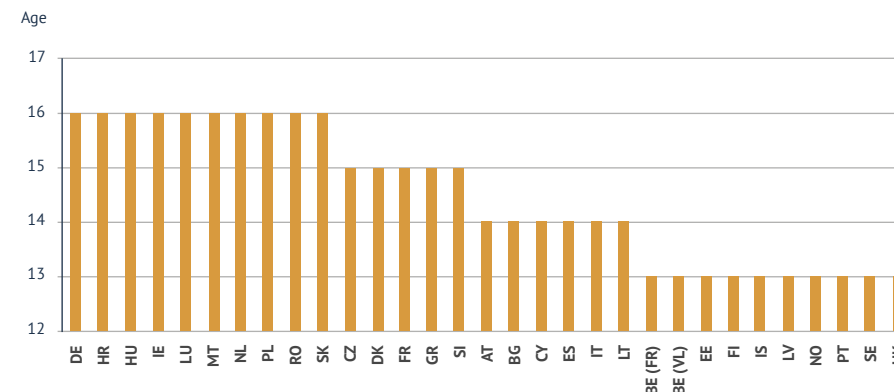
3.3.2 Minimum age for VSP access

In the absence of legislation stating otherwise, most VSPs have set a minimum age of 13 years for unsupervised access to their service.

In the EU, Article 8 of Regulation 2016/679, also known as the General Data Protection Regulation⁵ (GDPR), imposes a minimum age of 16 for the processing of data, with the possibility for member states to set a lower age, though not below 13.

In many EU member states, however, in application of the GDPR, national legislations set a higher minimum age for unsupervised access to VSPs. Although they impact VSPs, these rules are often found in legislation related to data protection rather than in media laws.

Fig 5. Minimum age for unsupervised access to VSPs according to data protection legislation



Source: The protection of minors on VSPs: age verification and parental control, European Audiovisual Observatory, Strasbourg, 2023

⁵ <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

3.4 Parental control (Article 28b(3)(h) AVMSD)

Article 28b (3)(h) AVMSD introduces the obligation for VSPs to put in place parental control systems:

“ (h) providing for **parental control systems** that are under the control of the end-user with respect to content which may impair the physical, mental or moral development of minors; ”

As is the case with reporting and flagging mechanisms and age verification, there are differences in national transpositions of Article 28b(3)(h) AVMSD.

KEY FACTS

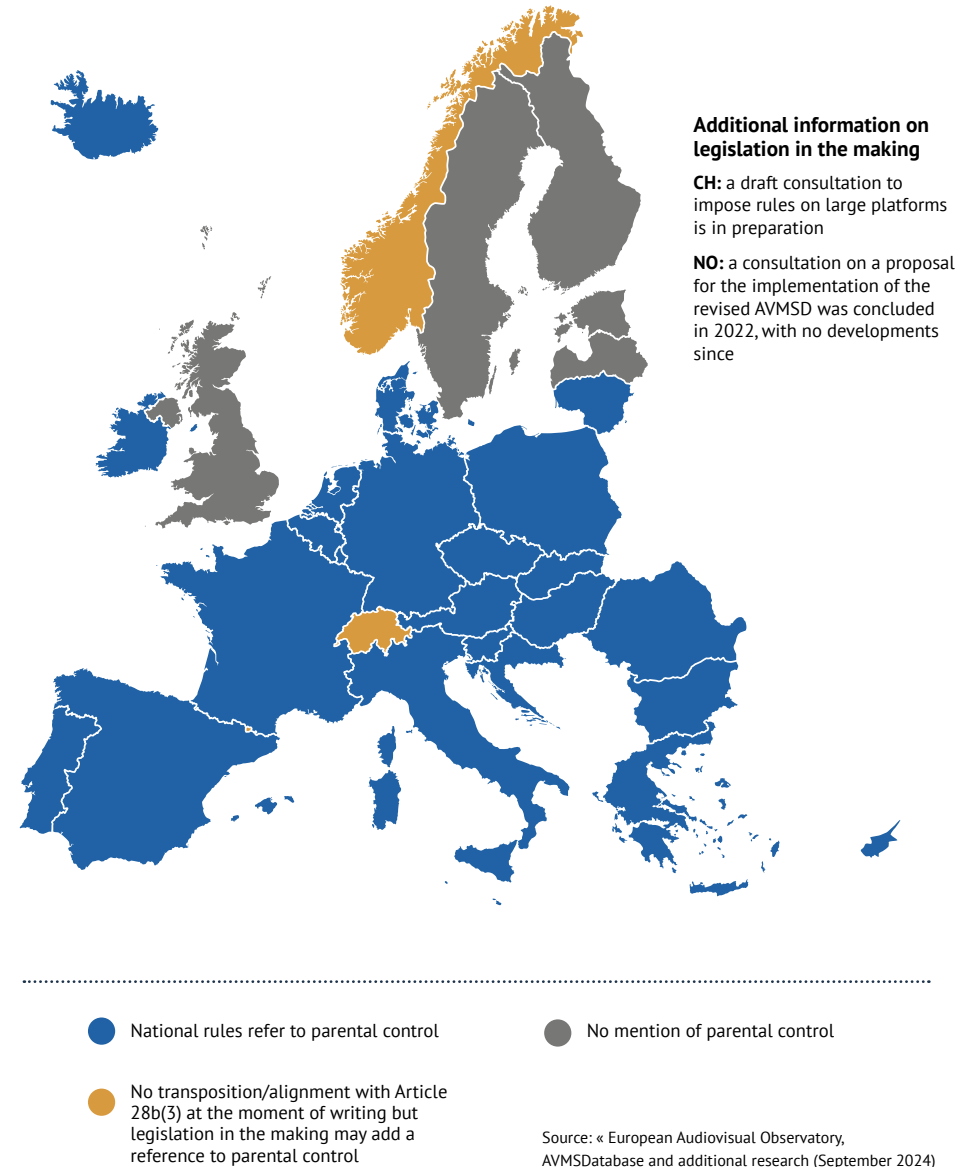
→ 22 EU member states reference parental control systems as one of the measures to be implemented by VSP providers, if appropriate, to protect minors.

→ National transpositions make no reference to parental control systems in EE, LV, NL and SE.

→ In the UK, parental control systems are not mentioned in the Online Safety Act 2023 either.

→ EFTA countries (with the exception of IS) have not yet transposed Article 28b (3) into their national legislations and make no mention of parental control systems to protect minors on VSPs.

Fig 6. National rules regarding parental control (Article 28b(3)(h) AVMSD)



Overview of national transpositions of AVMSD rules regarding parental control:

Countries with verbatim and substantially literal transpositions of Article 28b(3)(h) AVMSD

BE(DE), BE(FR), BG, CY, CZ, DK, DE, ES, GR, HU, HR, IE, IS, IT, LT, LU, MT, PT, RO, SI, and SK

Countries with more detailed transpositions of Article 28b(3)(h) AVMSD VSP providers shall:

AT	Federal Act on Audiovisual Media Services (AMD-G) Consolidated 1st January 2021 - Art. § 54e. 3.	Ensure that content that can impair the physical, mental or moral development of minors is solely provided in such a way that it cannot normally be viewed by minors, for instance with parental control systems, and such content can be assessed by users with a clear and easy to operate function. Access to content with gratuitous violence and content confined mainly to the unreflective depiction of sexual activity must in any event be subject to effective access control through parental verification.
BE(FR)	Flemish community - Decree on radio and television broadcasting Consolidated 1 December 2022 - Art. 176/6	Provide systems for parental control managed by end users for programmes, user-generated content and commercial communications which could be detrimental to the physical, mental or moral development of minors

Countries with broader transpositions of Article 28b(3)(h)

FR	Law No. 86-1067 of 30 September 1986 on the freedom of communication (Loi Léotard) Consolidated 18 August 2022 - Art. 60 II	Put in place age verification and parental control systems.
PL	Broadcasting Act Consolidated 21 April 2022 - Art. 47p	VSPs shall establish and operate effective technical safeguards, including parental control systems or other appropriate means of protecting minors from accessing programmes, user-generated videos or other communications prejudicial to the proper physical, mental or moral development of minors, in particular including pornographic content or showing gratuitous violence;

3.5 Protection of minors' data (Article 28b(3), final § AVMSD)

The last paragraph of Article 28b(3) AVMSD refers to the personal data of minors:

“ Personal data of minors collected or otherwise generated by video-sharing platform providers pursuant to points (f) and (h) of the third subparagraph shall not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising. ”

Similarly to the other measures that are mentioned in Article 28b(3) AVMSD, transpositions of the final paragraph come in different forms. In a majority of EU member states, the personal data of minors collected or generated by VSP providers cannot be used for commercial purposes, often transposing the AVMSD verbatim. A few EU member states do not specifically forbid the use of minors' data for commercial purposes, although they still refer to the wider idea that VSP providers must take measures to ensure that minors are protected from commercial communications as well as programmes and user-generated videos that could be detrimental to their development.



KEY FACTS

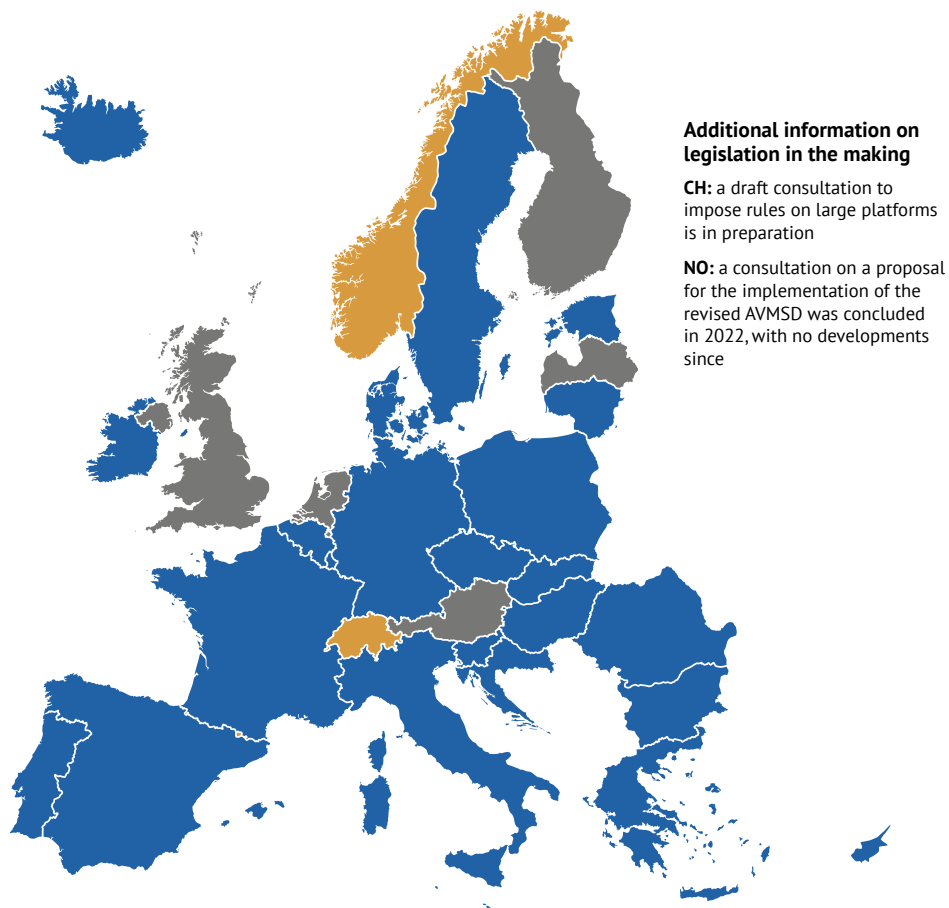
→ 23 EU member states forbid the use for commercial purposes of minors' data collected and/or generated while using VSPs.

→ National transpositions make no reference to minors' data in AT, BE(VL), FI, LV, and NL.

→ In the UK, the use of minors' data is not mentioned in the Online Safety Act 2023 either.

→ EFTA countries (with the exception of IS) have not yet aligned their national legislations with the dispositions of Article 28b (3) AVMSD and make no mention of minors' data.

Fig 7. National rules regarding the protection of minors' data (Article 28b(3), final § AVMSD)



- National rules refer to the protection of minors' data
- Legislation in the making may add a reference to the protection of minors' data based on the EAO's research and publicly available data

- No mention of the protection of minors' data

Source: European Audiovisual Observatory, AVMSDatabase and additional research (September 2024)

Overview of national transpositions of AVMSD rules regarding the protection of minors' data:

Countries with verbatim and substantially literal transpositions of Article 28b(3), final §, AVMSD

BE (DE), BE(FR), BE (VL) BG, CY, CZ, DK, DE, EE, ES, GR, HR, HU, IE, IS, IT, LT, LU, MT, RO, SK, SI and SE

Countries with more detailed transpositions of Article 28b(3), final §, AVMSD Summarised measures

FR	Law No. 86-1067 of 30 September 1986 on the freedom of communication (Loi Léotard) Consolidated 18 August 2022 - Art. 60 III	Personal data of minors collected or generated by VSP providers must not, even after those concerned reach the age of majority, be used for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.
PL	Broadcasting Act Consolidated 21 April 2022 - Art. 47p, 47r, 47s 1. and 47w	Personal data in relation to minors collected or otherwise generated by VSP providers shall not be processed for commercial purposes such as direct marketing, profiling, behaviourally targeted advertising, or other forms of commercial communications targeting audience groups selected by the provider, and used for those purposes in providing that platform, other VSPs or media services.
PT	Law 27/2007, of 30th July - Television and Audiovisual On-Demand Services Law Consolidated 19 November 2020 - Art. 93-B	Personal data of children and young people collected or generated by television programme service operators, on-demand audiovisual service operators or VSP providers shall not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.

4

ENFORCEMENT



4.1 NRA assessments according to the AVMSD

Article 28b (5) AVMSD

“ Member States shall establish the **necessary mechanisms to assess the appropriateness of the measures** referred to in paragraph 3 taken by video-sharing platform providers. Member States shall entrust the assessment of those measures to the **national regulatory authorities or bodies.** ”



ASSESSING MEASURES IN PRACTICE

- The appropriateness of the measures taken by VSP providers is assessed by the NRA of the country of establishment.
- This assessment process requires the NRA to follow a series of steps which are all essentially designed along the same lines.
- In order to enable the NRA carry out its enforcement tasks and in accordance with Article 28a(6) of the AVMSD, member states must draw up and keep up to date a list of VSPs established or deemed to be established on their territory. In this context, member states may organise notification/registration systems for VSPs.
- Following its assessment and if an infringement is found, the NRA may require VSP providers to adapt their measures and comply with the rules.
- If the request is not complied with, VSP providers may be subject to financial and/or other types of sanctions.

4.2 Status of VSP registration in the MAVISE database



KEY FACTS

The number of VSPs registered in Europe varies significantly between countries.

The differences are primarily driven by:

- 1 • the number of national VSPs
- 2 • whether the country is also acting as a hub for international VSPs
- 3 • the degree to which the legislation regarding VSPs has been implemented in the respective country of origin

Almost half of the registered VSPs provide adult content, a proportion that is expected to increase in the future.

VSPs presented in the table below are registered with the NRAs except for Luxembourg, where the registering body is the Luxembourg Deputy Minister for Communications.

Methodology:

MAVISE covers all VSPs registered in EEA and non-EEA countries which provide the Observatory with information.

In the same way as for TV channels and on-demand services, the Observatory complements the information on VSPs with desk research to identify the most prominent VSPs available in Europe that are not yet (or no longer) registered.

4.3 How NRAs assess the measures put in place by VSPs

The assessment of measures put in place by VSPs is entrusted to the NRAs or bodies in each country, to enforce the requirements set out in the AVMSD. Article 28b(5) is transposed rather literally into national law, which generally recalls the same general principles:

→ Prohibition of *a priori* assessment:

the NRA must ensure measures do not lead to any ex ante control or upload filtering of content.

→ Ensure that measures are appropriate and proportionate to achieve the intended aims, taking into account various factors:

the *nature* of the content in question, the *harm* it may cause, the characteristics of the *category of persons* to be protected as well as the *rights and legitimate interests* at stake, including those of the VSP providers and the users having created or uploaded the content as well as the general public interest. The NRA is also to take the size of the VSP and the nature of the service provided into account.

More specific information on the modalities of assessment and the powers of NRAs is usually found in secondary legislation, such as decrees or guidelines. This allows for more detailed implementation of the principles laid down by law, while leaving room for adaptation to national specificities. NRAs therefore play a key role in ensuring that audiovisual rules are enforced in a balanced manner.

Fig 8. Snapshot of VSPs registered in the national registries of the EEA countries and the UK

Country	Nbr	Examples	Country	Nbr	Examples
AT	2	Amateurseite	HU	10	Videa, Indavideó
BE	1	ItemFix	IE	10	YouTube, FB, Insta, Twitter, TikTok
BG	1	vbox7	LU	16	MyCams, LiveJasmin
CY	4	Pornhub, Stripchat, xHamster	NL	1	Snapchat
CZ	6	XVideos	PL	14	Wiocha, Hopaj
DE	1	Twitch	PT	4	Sapo Videos
ES	15	Canalporno, Porn300	SE	2	SwebbTube
GB	21	TikTok, OnlyFans, Twich, Vimeo, Snapchat	SK	1	Niké Fond športu

Source: European Audiovisual Observatory, MAVISE database (September 2024)

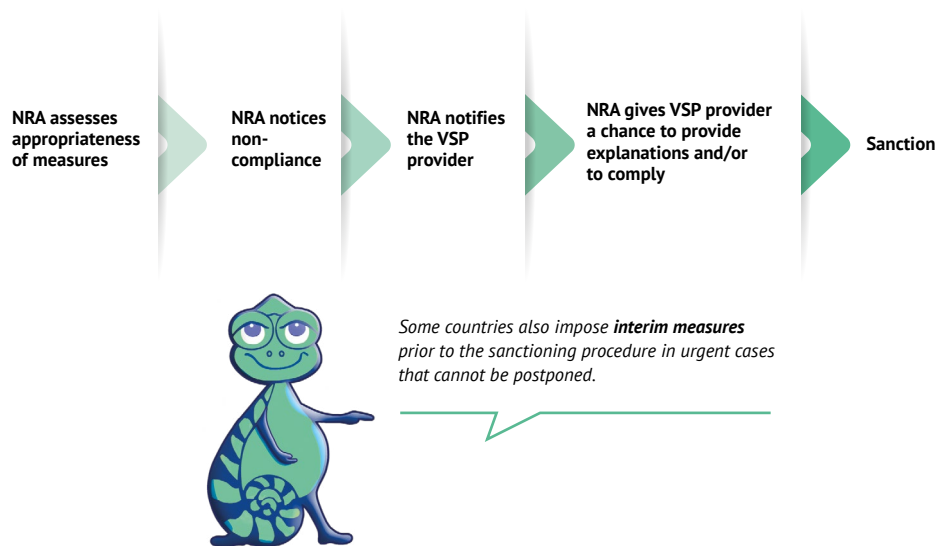


Finland requires a monitoring fee collected by the NRA, the National Audiovisual Institute (KAVI) to cover the costs of monitoring the provision of audiovisual programmes and VSP services. The fee is charged for the first time for the calendar year in which the provision of audiovisual programmes commences and amounts to EUR 400 for VSP services.

4.4 Request for adaptation

Under the national legislation of most of the countries covered by this report, if the competent NRA considers that the measures taken by a VSP to protect minors are not sufficient, it may notify the VSP provider and give it an opportunity to provide explanation or/and to comply with the measures required. If they fail to do so, the NRA generally has the power to impose sanctions.

Fig 9. Chronology



In **Spain**, the NRA may decide to **cease** the dissemination of the programme or content, or to **warn the public** about the matter. In addition, once the sanctioning procedure has been initiated, provisional measures may be adopted, consisting of an immediate **cessation** of the allegedly infringing activity, **confirmation or modification of the provisional measures** previously adopted for a maximum period of three months, which may be extended for a further period of up to three months, or, in the case of very serious infringements, **provisional suspension of the effects of the authorisation and provisional closure of the installations**.

4.5 Sanctions

By enforcing compliance, most NRAs have the power to sanction VSPs which fail to comply with the measures for the protection of minors. Sanctions most often take the form of fines but can also have a direct impact on distribution and access of content. Some countries require one or the other, or both.

All countries have implemented sanctions which can be applied to VSPs. Some countries have implemented additional specific sanctions in response to infractions relating to the protection of minors.



Sneak peek: Financial sanctions for specifically failing to protect minors

Country	Amount	Detail
IT	Between EUR 30 000 and EUR 600 000 or up to 1% of the annual turnover, when the value of such percentage exceeds EUR 600 000 of the turnover achieved in the previous financial year before the notification of the contestation.	These fines apply in cases where VSPs have failed to implement measures to protect minors.
PT	Very serious administrative offense: between EUR 75 000 and EUR 375 000	Fines are divided into minor, serious and very serious administrative offenses. Very serious administrative offenses include failing to comply with measures for the protection of minors.
SK	Between EUR 2 500 and EUR 100 000 for breaching the prohibition on the processing of personal data of minors	Fines depend on the type of infringement and whether the content provider requires authorisation or not.

Other types of sanctions

Alternatively, or in addition to financial sanctions, NRAs may impose other types of sanctions which may have a direct impact on the distribution of the content, on the VSP provider's authorisation to provide programmes and user-generated content, on the public's access to the content or on the public's awareness of the detection of infringements.

Such sanctions may include:

- Warning
- Reprimand
- Publication of a statement about the infringement
- Publication of the infringement decision
- Suspension or withdrawal of the offending programme/content
- Suspension or revocation of the authorisation/licence
- Suspension of distribution of the infringing service



FOCUS

Cross border cases

VSPs often operate across multiple countries while being established in one.

What is the issue? Platforms that serve users across the EU can trigger cross-border challenges, which is especially

relevant for the protection of audiences, and particularly minors. To tackle this issue, Italy has implemented rules allowing its NRA to take action over VSPs established abroad.



That is why cooperation between NRAs is of great importance!

Example. More protection for Italian users

On 22 November 2023, the Italian Communications Authority (AGCOM) adopted a regulation in line with Article 3, paragraphs 4 and 5 of the E-Commerce Directive, establishing rules aimed at protecting minors and consumers from harmful content on VSPs (Resolution no. 298/23/CONS) and allowing AGCOM to **restrict the circulation of content, even if VSPs are established abroad**.

To this end, at least one of the following criteria must be satisfied:

- Predominant use of the Italian language,
- Reach of a significant average number of unique monthly users in the Italian territory,
- Revenues achieved in Italy, even if accounted for in the financial statements of companies based abroad.

Two intervention methods:

- Notification to competent authority but if it does not act within seven days or if the action taken appears inadequate, **AGCOM can issue the order directly to the platform**.
- **In urgent cases**, AGCOM can intervene directly and immediately, and **order the platform to block access** to content within three days.

First case implementing the regulation of VSPs

AGCOM noted the presence, on TikTok, of "French scar" videos consisting of continuously and violently squeezing the skin of the cheeks to the point of bruising the cheekbones.

In accordance with the regulation on VSPs, AGCOM initiated an intervention procedure leading TikTok, a VSP based in Ireland, to remove the videos.

5

VSP MEASURES IN PRACTICE



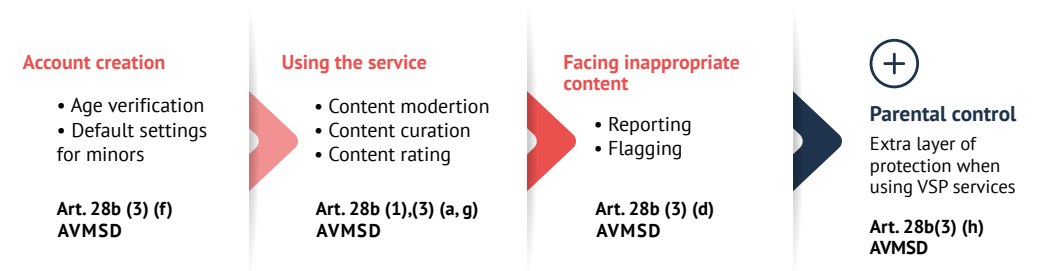
5.1 Introducing the measures

This chapter explains how the rules presented in the above chapters are implemented in practice by six VSPs (Facebook, Instagram, Snapchat, TikTok, X (formerly Twitter), and YouTube) which have also been designated as VLOPs under the DSA.⁶

All six platforms have implemented protective measures with regard to minors and their approaches vary. Some platforms have standard protective measures, while others implement more extensive systems of protection.

Fig 10. What steps should a minor take to access content on a VSP?

To access content on a VSP, minors need to follow a series of steps from creating an account to using the service and knowing how to flag inappropriate content:



Source: EAO elaboration, September 2024

⁶ The analysis is based on the platforms' terms and conditions and community guidelines, accessed from France in September 2024, along with the EAO's understanding of these practices.

Account creation

Age verification measures, as provided by Article 28b(3)(f) AVMSD, are in place to ensure the account owner is of the minimum age required by their member state:⁷

→ Registration usually involves providing personal information, such as a username, email address, and sometimes a birthdate to confirm age. Many platforms require users to be at least 13 to create their own account (or older, depending on the minor's geographical location), depending on the platform. In some cases, parents/guardians may need to give consent.

→ To obtain consent, methods may include sending an email to a parent/guardian, or verifying credit card information.

→ Default settings apply based on the minor's birth date to ensure additional protection of their account.



Content hosted by platforms is sometimes visible to all from a desktop without logging in; this is usually the case for non-sensitive content.

Using the service

While accessing content and feeds of activities, minors should be protected from content which may impair their physical, mental or moral development (Art. 28b(1) AVMSD). In practice, VSPs can moderate and curate content by using algorithms, filters, recommendation systems, etc. VSPs can also rate content based on minors' age to determine whether minors should see (or not) a specific content:

→ Accessing content involves browsing, searching and exploring different sections of the platform, following creators and subscribing to channels. Minors can watch videos, comment, like, or share content. Platforms often have guidelines and community rules to ensure appropriate behaviour.

→ Age-appropriate measures allow platforms to offer minor-appropriate content or limit minors' exposure to sensitive content. Minors may need to adjust settings or rely on parental controls to ensure these settings apply.

Flagging content

When minors face content they should not encounter, a mechanism should allow them (and/or guardians) to report or flag to the VSP the said content (Art. 28b(3) (d) AVMSD).

→ Reporting/flagging inappropriate content generally involves clicking a "report" or "flag" option and choosing a reason for the reporting.

→ By seeking assistance, minors may involve a parent, guardian, or teacher if they encounter problematic content or behaviour on the platform.

Fig 13. Non-exhaustive examples of practices implemented by VSPs (covering Art. 28b (1), (3) (a, d, f, g, h, and last paragraph AVMSD):

	Measures	Facebook	Instagram	Snapchat	Tiktok	X	YouTube ⁸
Account creation	Indicate birth date ⁹	●	●	●	●	●	●
	Settings for minors apply by default	●	●	●	●		●
	Investigation of a minor's account suspected to be under-aged	●	●	●	●	●	●
Using the service	Promotion of content which is most relevant to the user	●	●	●	●	●	●
	Content adapted to minors' age based on the birth date	●	●	●	●	●	●
	Additional protection with parental control measures	●	●	●	●		●
Flagging content	Reporting problematic content by clicking a button next to the content	●	●	●	●	●	●

Source: EAO elaboration, September 2024

7 As provided for in the GDPR, which sets a minimum age of 16 for the collection of minor's data but allows member states to lower this minimum age to 13. In many cases, an account can be created for minors who are at least 13 years old.
 8 Minors under 13 are redirected to YouTube Kids (restricted account for kids with specific default settings, to be set up by a parent)
 9 Some services block the possibility for minors between 13 and 17 to modify their birth date to appear older once they have created their account.

5.2 Account creation: step 1 - age verification

What is age verification?

While there is no definition in the AVMSD of “age verification systems” despite a provision requiring the VSPs to enforce age requirements (Art. 28b(3)(f) AVMSD), the European Commission’s website on the AVMSD and minor protection refers to systems that prevent minors from seeing programmes that may impair their development.¹⁰ This can be done using PIN codes or other more sophisticated age verification systems.

For the six VSPs, age verification systems are set up to ensure minors are of the required minimum age to access the service. When this is not the case, the minor alone should not be able to create their account. In addition, being aged between 13 and 16 years old can lead, on some VSP services, to additional verifications to ensure the safety of minors.

Fig 14. Age verification in practice: common systems

1 Birth date

- Min 13 years old to sign up alone.
- If the date of birth provided indicates the user is under 13, impossible to sign up alone.
- Many VSPs remember the email address and/or IP address used during the account creation, preventing creation if a different birth date is later entered from the same source.
- Some VSPs do not allow minors between 13 and 17 to modify their birth date in the settings once they have created their account. This may trigger default settings and parental control.

2 Account review

- Users suspected to be underage: the account can be flagged by other users or by VSPs and put under review.
- VSPs conduct an investigation to determine the user’s age.
- If the suspicion is confirmed, VSPs require further age verification. This verification could involve a facial analysis estimate, either alone or with an adult’s assistance. If the user is found to be underage, the platform may delete the account.

3 Further age verifications

- If a user is suspected of being underage, the VSP may request additional verification within a specified time frame (eg. providing an ID and a selfie of the minor holding the ID along with a code provided by the platform).
- If the user is between 13 and 17 years old, the verification may involve an adult too (min 25 years old) accompanying the child (eg. the adult must hold a paper indicating their age, the child’s birth date, and the code provided by the platform.)
- Alternatively, age verification can also be done with a credit card.

4 Account deletion

- If the user fails to meet the minimum age requirement to have their own account, the account will be deleted, along with any associated data.



These initial steps of age verification when creating an account may lead to default settings that provide additional protection for minors.

Source: EAO elaboration, September 2024

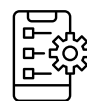
¹⁰ <https://digital-strategy.ec.europa.eu/en/policies/avmsd-protection-minors>

5.3 Account creation: step 2 - default settings

Default settings for minors: what are they? After filling in their birth date, VSPs may apply, by default, settings for minors. They typically prioritise a higher level of privacy when minors use the platform’s services.

Default settings generally apply to users aged between 13 and 16 (or 17) years old. They are organised into specific categories that focus on user experience and safety. The following measures are based on the most common default settings across the six VSPs studied:

Fig 15. Clusters of most common default settings for minors that automatically turn on when signing in:



Activity monitoring and privacy settings allow to:

- Limit who can see their friends list
- Know who can see the people, pages, and lists they follow
- Know who can see posts they’re tagged in on their profile
- Review posts they’re tagged in before the posts appears on their profile
- Know who is allowed to comment on their public posts
- Turn off location sharing by default; location sharing, if used, can only be with friends
- Silence push notifications at night
- Disable direct messaging



Communication settings allow to:

- Limit communications to friends and phone contacts



Account supervision and security allow to:

- Recommend that minors enable two-factor authentication
- Verify their email address and phone number to prevent hacking and protect personal information



Time management allows to:

- Limit screen time per day

Fig 16. Age up to which default settings for minors are enabled:

Facebook Instagram	→ 16 years old
Snapchat Tiktok	→ 17 years old
YouTube	→ YouTube Kids for kids under 12 with limited choices of content. The account is supervised by an adult. Above 13 years old (or more depending on the country), the minor is deemed free to use YouTube services. Parents can still supervise the account, with specific content settings.
X	→ Users must be minimum 13 years old to use the service unsupervised

5.4 Using the service: ensuring minors see appropriate content only

In practice, how can VSPs ensure that minors do not see content which may impair their development? By including and applying in their terms and conditions the content requirements set out in Article 28b(1)(a) AVMSD, in line with Article 28b(3)(a) AVMSD. VSPs apply their terms and conditions through content curation, moderation and rating. Content moderation is now defined in the DSA under Art. 3(t) and encompasses activities, whether automated or not, carried out by intermediary service providers to detect, identify, and manage illegal content or information that violates their terms and conditions. In practice, content curation, moderation and rating may intervene concurrently and may go unnoticed by minors.

Fig 17. Content curation, moderation and rating:

Content curation

Involves personalising the content users see based on their behaviour and preferences. Recommendation systems and filters play a big role here. As minors specify interests when creating an account, algorithms learn from these interactions to show them content that's tailored to their interests (default settings, birth date and minors' own likes individualise what they see too). This helps individualise experiences while promoting age-appropriate content.

In practice, categorisation allows for the personalisation of content suggestions. It ensures that minors i) access content they like and ii) do not see inappropriate content.

Content rating

Is a mechanism that ensures age-appropriateness of the content. Based on the birthdate provided by users when creating accounts, platforms can limit access to certain content for those below a specific age. Content intended for users over 18 is often flagged or restricted, ensuring a boundary for minors.


Content rating confirms the content is fit for a certain public, based for instance on the age of the potential audience.

Content rating may lead to blocking access to minors.

Content moderation

Involves the ongoing tracking and filtering of content to ensure it aligns with the VSP's community guidelines and is safe for minors. This can be achieved through automated algorithms that detect and flag inappropriate content, as well as manual reviews.

It detects and identifies (in)appropriate content and ensures minors only access content that may not impair their development.

 Although these measures aim to ensure minors have access to content that is appropriate for their age, the definition of what is appropriate for minors is not always clearly defined in law. The only established legal guideline is that content should not impair their physical, mental, or moral development, as outlined in Article 6a(1) AVMSD.

- 1  **Inappropriate only for minors**
If the content is only inappropriate for children, VSPs should filter the content and ensure it does not appear in minors' feeds.
- 2  **Content against VSPs' terms and conditions**
Identified content, usually goes under a human review after it has been algorithmically flagged. The content is deleted.



Content curation, moderation and rating are systems that help VSPs create a safe experience for minors. Let's break these terms down and provide examples of how some VSPs implement these measures.

Non-exhaustive practical examples based on VSPs' terms and conditions:

- Meta** → ranks content to promote posts and comments which are the most relevant to minors.
- Snapchat** → uses detection tools to identify public accounts that promote age-inappropriate content. A system of sanctions is in place to deal with these accounts, preventing minors from accessing harmful material.
- Tiktok** → moderates LIVE content by restricting access to minors if the content is deemed inappropriate for users aged 13 to 17. If such content is detected, it will not be recommended to this audience, and underage viewers are disconnected from the stream. This category of users is also prevented from accessing LIVE sessions via search or shared links.
- X** → restricts the visibility of specific forms of sensitive media, like adult content, to users under 18. This helps ensure that young users are not exposed to inappropriate content.
- YouTube** → limits access to certain content (e.g. violent or pornographic content) to users over 18 who have signed into their accounts (provided the content is appropriately categorised). If such content hosted by YouTube is embedded on another website, users are redirected to YouTube to verify their age before they can watch it. This system ensures that age restrictions are enforced even when content is shared externally.

5.5 Additional layer of protection with parental control

Parents and guardians can play a role in ensuring the safety of their children in the digital world. VSPs offer a variety of parental control functions to help adults monitor, manage, and restrict content, communications, and other features. These functions may vary across platforms and aim at complying with Article 28b(3)(h) AVMSD, which requires VSPs to offer parental control systems. Here are some of the types of parental control functions across the six VSPs under review:

→ **Activity monitoring and time management** for parents and guardians to track minors' app usage, to set time limits and to schedule breaks to manage screen time;

→ **Communication settings** for parents and guardians to oversee and limit who can communicate with minors through direct messages, comments and group chats;

→ **Content management and filtering** for parents and guardians to have control over the content minors can access (i.e. content restriction, filtering keywords, and managing browsing permissions);

→ **Account supervision and security** for parents and guardians to manage privacy settings, oversee account security and verify age requirements.

Each VSP provides its own set of features ensuring parents have tools to help minors safely enjoy online content. Parental control measures are applicable when minors are aged between 13 and 17. It is often up to the parents to make use of these “family centres” and turn on the various measures offered to them.

Fig 18. Examples of tools parents/guardians can use:



Activity monitoring and time management

- Track usage time,
- Set (daily) time limits,
- Schedule breaks,
- Remotely lock services during specific times

VSPs using some of the above examples:

Facebook, Instagram, Snapchat, TikTok, YouTube



Content management and filtering

- View minor's friends,
- See content preferences,
- Restrict sensitive content,
- Report abuse,
- See account-related details, such as who minors follow and who they have blocked,
- Filter keywords and hashtags,
- Block or allow certain sites

VSPs using some of the above examples:

Facebook, Instagram, Snapchat, TikTok



Communication settings

- Manage direct messaging access and who can add minors to group chats,
- Manage who can comment on videos,
- See who minors message,
- Silence push notifications

VSPs using some of the above examples:

Facebook Messenger, Instagram, Snapchat, TikTok



Account supervision and security

- View and control some privacy settings,
- Parents/guardians receive notifications if some setting changes are made.

VSPs using some of the above examples:

Facebook, Instagram, Snapchat, TikTok, YouTube

Source: EAO elaboration, September 2024

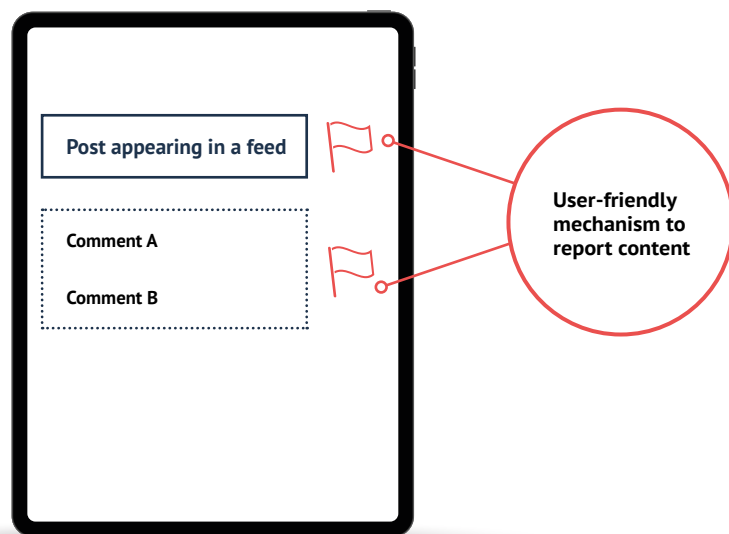
For parents/guardians to use parental control tools, some VSPs may require parents to install the VSP's app on their own device to oversee their child's activity.

5.6 Reporting and flagging content

VSPs must provide users with simple, user-friendly tools to report or flag content that might negatively impact minors' physical, mental, or moral development, as provided for by Article 28b(3)(d) AVMSD. Every platform examined in this study has integrated user-friendly mechanisms for reporting such content. These systems are designed not only for age-inappropriate material but also for any content that violates the platform's terms of service, community guidelines, or other rules. This system encompasses videos, comments, live streams, live comments, user accounts, and more.

Typically, users can report problematic content by clicking a button adjacent to the content, either in the app or on a web browser. Some platforms also offer a separate form for additional reporting.

After a report is submitted, the platform will analyse the content, whether through automated processes or human review, and remove it if it violates the platform's terms of service, community guidelines, or other rules.



Thanks for staying with us. We hope that you found the content of this report interesting

If you would like to know more about VSPs, have a look at our mapping on the rules applicable to VSPs for illegal and harmful content online:

<https://rm.coe.int/mapping-on-video-sharing-platforms-2022-update/1680aa1b16>

You will also find a lot of data on the rules applicable to VSPs with a focus on commercial communications in this specific mapping:

<https://rm.coe.int/mapping-on-video-sharing-platforms-2022-focus-on-cc/1680aa1b15>

If you want to know more about age verification and parental control measures on VSPs, check our AVMSD Note here:

<https://rm.coe.int/the-protection-of-minors-on-vsps-age-verification-and-parental-control/1680af0788>

European Audiovisual Observatory

76 Allée de la Robertsau – 67000 Strasbourg – France

Tel: +33 (0) 3 90 21 60 00

www.obs.coe.int

