Coimisiún na Meán

Call For Inputs: Online Safety

Developing Ireland's First Binding Online Safety Code for Video-Sharing Platform Services

Publication Date: 11th July 2023

Coimisiún na Meán

Legal disclaimer

This is a call for inputs document intended to invite submissions to inform a future consultation by Coimisiún na Meán (the “Commission”) on a draft Online Safety Code. The Commission is not taking definitive positions on issues at this time and this Call of Inputs should not be read as reflecting or stating the Commission's position on any matter. The subject area is complex involving different legal instruments; we have aimed to improve the accessibility of this document for stakeholders not familiar with its subject matter. Please note that any views on the interpretation of legislation or the Commission's obligations are provisional and non-binding and should not be read as reflecting the Commission's final position. Please refer to the underlying legislative provisions for a statement of the law in this area.

Coimisiún na Meán

Contents

Coimisiún na Meán

1. Introduction

Coimisiún na Meán (the "Commission") is Ireland's regulator for broadcasting, on-demand and online safety. The Commission was established in March 2023 further to the Broadcasting Act 2009 as amended by the Online Safety and Media Regulation Act 2022 (the "2009 Act as amended").[1] We have a range of responsibilities, and these include setting standards, rules and codes for the different types of media services and relevant online services under the jurisdiction of the Irish State. We will also be Ireland's Digital Service Coordinator (DSC) under the EU Digital Services Act 2022 (the "DSA").[2]

One of the Commission's key duties under the 2009 Act as amended is to develop online safety codes for video-sharing platform services ("VSPS").[3] A VSPS is a type of online service where users can share videos and engage with a wide range of content and social features.[4] The definition includes popular social media services where user-generated videos are available but excludes private messaging. We intend for the first Online Safety Code to focus on VSPS providers and make sure they take measures to address online harms more effectively.[5] We intend to design the Code to ensure that the Commission meets its obligations under the 2009 Act as amended to develop such a code and to ensure that Ireland fully transposes Article 28b of the revised Audiovisual Media Services Directive (the "AVMSD").[6] This Directive coordinates EU-wide rules for national legislation on audiovisual media — traditional television broadcasts, on-demand services and VSPS.

The Commission is currently in a stage of information-gathering and reflection prior to preparation of draft legal measures and formal consultation on those. As part of this process, we are now seeking your input on how we should develop Ireland's first binding online safety code (the "Online Safety Code" or the "Code").

This document explores the potential scope of the Code and sets out a range of questions that we would like you to consider. Your responses will play an important role in helping us to identify issues and information that we can take into account when developing the Code, to the extent that they are in line with our legal powers and obligations. We will publish a draft Code later in the year and will consult formally on the draft before finalising it and applying it to VSPS.

---

[1] See https://www.irishstatutebook.ie/eli/2022/act/41/enacted/en/print.html.
[2] We will be officially appointed as Ireland's Digital Services Coordinator when the Digital Services Bill is agreed by the Houses of the Oireachtas. Further information about the Digital Services Act and the Digital Services Bill can be found here: General Scheme of the Digital Services Bill 2023 - DETE (enterprise.gov.ie)
[3] Please refer to Section 139K(3) of the 2009 Act as amended.
[4] Please refer to section 2 of the 2009 Act as amended for the precise definition as set out in statute.
[5] In this document we are using the terms 'online harms' and 'online harm' to capture the harm that can be caused by harmful online content, illegal content, inappropriate content and commercial communications collectively.
[6] Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services as amended by Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018.

We are also taking a number of other steps to help develop the Code. These include: -

1. Developing an e-Commerce Compliance Strategy – The Commission will consult on and adopt a strategy to ensure that the Code complies with Section 139ZF of the 2009 Act as amended;

2. Establishing a Youth Advisory Committee – The Commission intends to establish this Committee pursuant to Section 19 of the 2009 Act as amended. The Youth Committee will advise the Commission on its online safety work as that work relates to the interests of children and people who are 25 years old and younger;[7]

3. Conducting research on online harms;

4. Designating VSPS – The Commission will consult on bringing VSPS within the scope of its regulatory framework for online safety including the Code.

This Call for Inputs is an important step towards developing Ireland's first binding Online Safety Code. We want to collect a wide range of views and use these to help develop a code that is fit for purpose and is clear, workable and legally robust. Most importantly, we want the Code to protect children and the general public from online harms while upholding and promoting human rights, including the right to Freedom of Expression. The two main ways we anticipate the Code will achieve this is by requiring VSPS providers to introduce online safety features for their users and to moderate content more effectively. We also want the Code to improve the transparency of online platforms, to address the impacts of automated content moderation, and to work proportionately and fairly for the services it regulates. We will take a child-centred approach to developing the Code where it impacts children.[8]

The Code will complement the Digital Services Act ("DSA") when this comes into full effect in February 2024. The DSA will also promote greater online safety and has a wider focus than the Code, which will relate to VSPS. We want the Online Safety Code and the DSA to complement each other and provide a high level of online safety for everyone.

Structure of the Call for Inputs

In terms of the structure of this document: -

- **Section 2** sets out how you can respond to the Call for Inputs.
- **Section 3** explores the online harms the Code is likely to cover.

[7] The committee shall include such representatives as may be nominated at the invitation of the Commission by organisations representing children or people of not more than 25 years of age. At least half of the members of the Youth Advisory Committee shall be not more than 25 years of age.
[8] The rights of the child are enshrined in Article 24 of the EU Charter for Fundamental Rights which provides that "In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration…" Article 3 of the UN Convention on the Rights of the Child requires putting the best interests of the child first in all actions concerning children.

- **Section 4** invites views on the overall approach we should take to developing the Code.
- **Section 5** explores the measures we may ask VSPS providers to take.
- **Section 6** sets out matters relating to Data Protection and Freedom of Information.
- **Annex 1** includes some indicative questions to support engagement with children and young people by groups and organisations representing their interests.
- **Appendix 1** contains non-exhaustive extracts of legislative provisions from the 2009 Act as amended and the AVMSD.

2. Responding to our Call for Inputs

The rest of this document sets out a number of issues and questions. It explores a wide range of topics, some of which are complex. We appreciate the audience for this document is very varied and do not expect all interested parties to respond to every question. You should feel free to respond to one or some or all the questions set out below. If you are an organisation engaged with, or representing, children and young people we would direct your attention to Annex 1. This includes information that may assist you should you have the opportunity to engage directly with children or young people on the Call for Inputs.

We request that submissions are concise and focus on the key points you wish to make. These should be made in the main part of your response rather than via any supplemental material you choose to provide. You should **clearly identify** the question or questions you are responding to and responses to each question should ideally be, on average, no longer than one page. You should provide any supplemental information in a single appendix. Where possible, research or other material should be identified using links in footnotes in the main body of your submission rather than in an appendix. It would be especially helpful if you could provide your evidence and opinions drawing on the criteria we have to consider when we prepare the Code (we have set out a non-exhaustive list at Appendix 1). We do not require you to send us examples of online harm. If you do wish to do so, a brief written description of the online harm will be sufficient.

Please remember that we are at an early stage in the process. This Call for Inputs is broad and we will take account of relevant submissions, together with additional information and evidence, when we are exercising our powers to develop a draft Code. We may not take account of all the information received in response to this Call for Inputs, to the extent that it is not relevant or not in line with our legal powers and obligations. We will publish a draft Code for consultation later in the year and you will have an opportunity to submit comments on the specific proposals at that time.

Your response can be submitted in writing by email or by post/hand to one of the following addresses:-

Email: VSPSregulation@cnam.ie **Contact Person:** Laura Forsythe

Post: VSPS Regulation, Coimisiún na Meán, 2-5 Warrington Place, D02XP29, Ireland.

All responses to this Call for Inputs must be submitted in writing to the Commission by **16th August 2023.** Responses received will be handled in line with our obligations and policies that relate to data privacy and freedom of information, and these are detailed in section 6 below.

If you require any assistance making a response, please contact the Commission by email to VSPSregulation@cnam.ie or by phone on 01 644 1200. Please mark confidential any information you require to be redacted on grounds of confidentiality and provide reasons for this.

3. Online Harms

In this section we are seeking views, information, and evidence about the online harms and issues you would like the first Online Safety Code to address. We have phrased our questions broadly because we would like you to identify and set out the issues about online harms that are most important to you.

You should not feel that you need to explore the legal elements of the questions we ask unless you would like to do so. When we consider your response to our questions in this section we will also consider how they tie into the more focused regulatory questions we ask about how we will design the Code in Section 4 and the specific measures for VSPS in Section 5.

3.1 What online harms should the Code address?

EU Member States must ensure that VSPS providers established in their jurisdiction provide the protections referred to in Article 28b of the AVMSD. In Ireland, we are responsible for making sure VSPS providers under the jurisdiction of the Irish State take these measures through Online Safety Codes.[9] Article 28b addresses harm in four main areas:

1. Content that might impair the physical, mental or moral development of minors. This includes content that may be inappropriate for children, such as pornography.

2. Content that incites violence or hatred against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the European Charter of Fundamental Rights. These grounds include sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

3. Content the dissemination of which constitutes a criminal offence under EU law. This includes:

    - Content that is a public provocation to commit a terrorist offence;
    - Offences concerning child sexual exploitation & abuse;
    - Offences concerning racism and xenophobia.

[9] See section 139(k) of the 2009 Act as amended.

4. Certain commercial communications that would not be permitted on broadcast or video-on-demand services.[10] Commercial communications include advertising, sponsorship and product placement.

Subject to consultation, we intend the Code to complete the transposition of Article 28b in Ireland by addressing online harms in these four main areas and by requiring VSPS to adopt the specific measures described in Article 28b.3 as appropriate (see section 5).

The 2009 Act as amended also specifies that we may address wider categories of harmful online content. The two wider categories include:

1. Harmful online content on services by which a person:[11]
    - Bullies or humiliates another person;
    - Promotes or encourages behaviour that characterises a feeding or eating disorder;
    - Promotes or encourages self-harm or suicide;
    - Makes available knowledge of methods of self-harm or suicide.
2. Harmful online content relating to 42 criminal offences under Irish law listed in Schedule 3 of the 2009 Act as amended.[12] Examples of offences include:
    - Non-consensual sharing of intimate images;
    - Child sex abuse material
    - Naming complainants in rape trials;
    - Material relating to suicide;
    - Harassment;
    - Child and human trafficking;
    - Domestic violence.

[10] This includes, among other things, requirements that commercial communications are transparent to users, do not include content that will cause physical, mental or moral detriment to minors, and meet standards in terms of human dignity, and non-discrimination. Restrictions on certain products and services are also included, such as alcohol, cigarettes, e-cigarettes and medicines.
[11] The content must give rise to a risk to a person's life or a risk of significant harm to a person's physical or mental health where the harm is reasonably foreseeable.
[12] Please refer to this link for the full list.

We have to decide what online harms the first Code for VSPS will cover. To transpose the Directive, it must address harm in the four main areas covered by Article 28b of the AVMSD. We also need to consider how we should use our code-making powers to address the types of harmful online content under the 2009 Act as amended.

Question 1: What do you think our main priorities and objectives should be in the first binding Online Safety Code for VSPS? What are the main online harms[13] you would like to see it address and why?

Question 2: What types of online harms do you think should attract the most stringent risk mitigation measures by VSPS? How could we evaluate the impact of different types of harms e.g. severity, speed at which harm may be caused? Is there a way of classifying harmful content that you consider it would be useful for us to use?

Question 3: Do you have reports, academic studies or other relevant independent research that would support your views? If you do, please share them with us with links to relevant reports, studies or research.

4. Overall Approach to the Code

In this section we are seeking your views on four key questions to inform the overall approach we take to designing the Code. These questions focus on how prescriptive or flexible the Code might be, its structure, its relationship with the DSA and how it should approach content connected to video content.

In section 5 we explore the "Appropriate Measures" we may ask VSPS providers to take in the Code. You may find it helpful to explore section 5 before considering and answering the questions in this section.

Please note that in this section we presume that we will adopt **one** Code for VSPS providers, at least initially. You are welcome to offer your views on whether you feel multiple codes could be a more effective approach, either on first adoption or later.

4.1 How prescriptive or flexible should the Code be?

We have to decide how prescriptive or flexible the Code will be.

Option 1 *– A very detailed, prescriptive Code*

The Code could specify in detail the measures we expect VSPS providers to take to address online harms.

[13] Please remember that when we refer to 'online harms' and 'online harm' in this document this includes harm that can be caused by harmful online content, illegal content, inappropriate content and commercial communications collectively.

Option 2 *– A very high-level Code*

The Code could set out categories of harm for VSPS providers to address and then oblige those providers to take appropriate measures to reduce the risk of harm in general terms.

Option 3 *– A mixed approach*

A middle way might be to impose high-level obligations and supplement them with more detail where appropriate. For example, the Code could include a high-level obligation that requires VSPS providers to have and to apply terms and conditions that prohibit users from uploading hate speech videos. The Code could then further specify that hate speech videos (or other videos) must be taken down within a specified time after being flagged.

We could supplement the Code with more detailed guidance to assist platforms with compliance. We could also require VSPS providers to be transparent about the measures they are taking to comply with high-level requirements and to provide metrics that would enable their effectiveness to be assessed.

Question 4: What approach do you think we should take to the level of detail in the Code? What role could non-binding guidance play in supplementing the Code?

4.2 How should we structure the Code?

We have to develop an appropriate structure for the Code. What will work best will depend on the harms it addresses and the regulatory approach we take to the issues it covers (see section 5). We have different options to consider.

For example:

- We could have separate sections in the Code for each main category of content it addresses.

- We could structure the Code thematically based on how the different parts of VSPS are impacted by the appropriate measures set out in Article 28b.3 of the AVMSD (See Section 5 below). For example, the Code could be split into the following sections: Content Policies / T&Cs; Risk Assessments; Content Moderation and Complaints; Online Safety Features; Service Design Measures; Compliance Measures.

- We could structure the Code by working through the Article 28b.3 measures of the AVMSD sequentially from (a) to (j) (See section 5).

- If we were to introduce a very high-level code it may only have one or two sections.

Question 5: What do you think would be the most effective structure for the Code? What are the most important factors we should consider when we decide how to structure the Code?

4.3 How should the Code take account of the Digital Services Act ("DSA")?

VSPS providers will have to comply with obligations for online platforms under the DSA and some may be subject to the additional obligations that apply to Very Large Online Platforms ("VLOPs").[14]

The Online Safety Code might impose additional and/or more detailed requirements on VSPS providers. For instance, the DSA contains a high-level requirement to protect the privacy, safety and security of minors. The Online Safety Code could impose more specific requirements in areas such as age verification/assurance, content rating, profiling of minors by recommender systems and parental controls.

We think it would be helpful to design the Code to minimise the potential for conflict and maximise the potential for synergies in how platforms comply with it and the DSA. One option would be for the Code to mirror or draw from the provisions of the DSA where possible. For instance, a platform is obliged to introduce a mechanism under the DSA that allows interested parties to notify it of illegal content and requires the platform to take action on receipt of a notice. The Code could require VSPS providers to extend this mechanism to cover certain types of harmful content. This might make it simpler for VSPS providers to comply with both the DSA and the Online Safety Code, with a single user experience and a single set of trust and safety practices.

The Code could also add more detail about how VSPS providers are obliged to comply. For instance, the DSA specifies that notices should be processed in a timely and diligent manner. The Code could specify metrics about the timing and accuracy of moderation decisions and actions in relation to particular categories of content. In your response to this question, you may also offer views on how you think we could design the Code to work effectively with other pieces of legislation in the content regulation space, such as the Terrorist Content Online Regulation (TCOR). [15]

Question 6: How should we design the Code to minimise the potential for conflict and maximise the potential for synergies in how platforms comply with it and the DSA?

4.4 How should the Code address content connected to video content?

Videos on VSPS are often provided with other forms of content which enhance and alter how users experience them, including, potentially, the harm they may cause. Comments posted by users who have viewed videos, descriptions of videos or text and images embedded with videos can change the impact they have. For example, a racist or antisemitic caption beneath a benign video can lead it to cause harm where it otherwise would not by making the video a vehicle to incite racist or antisemitic hatred.

We want the Code to robustly implement Article 28b of the Directive and we consider it appropriate at this stage to seek views on whether or not the Code should address content connected to video content.

[14] Under the DSA a VLOP is an online platform with a reach of at least 45 million active EU service recipients on average each month and which is designated as a VLOP or VLOSE (Very Large Online Search Engine).
[15] Regulation 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

Question 7: To what extent, if at all, should the Code require VSPS providers to take measures to address content connected to video content?

5. Measures to be taken by Video-Sharing Platforms

We have to ensure that VSPS providers take appropriate measures to protect the general public and children from online harms. What are the appropriate measures that they need to take? There is a non-exhaustive list of ten measures set out in Article 28b.3 of the AVMSD. These can be summarised as:

a) Ensuring their terms and conditions appropriately address harms to the physical, mental and moral development of minors; incitement to hatred and violence on EU charter grounds; and EU Criminal Offences. VSPS providers must apply these terms and conditions when relevant issues come to their attention;

b) Ensuring their terms and conditions are aligned with national rules to protect the general public from certain kinds of commercial communications which are not marketed, sold or arranged by the VSPS provider. VSPS providers must apply these terms and conditions when relevant issues come to their attention;

c) Having a functionality for users who upload user-generated videos to declare whether such videos contain commercial communications as far as they know or can be reasonably expected to know;

d) Establishing and operating transparent and user-friendly mechanisms for users of a VSPS to report or flag content to the platform provider;

e) Establishing and operating systems through which VSPS providers explain to their users what effect has been given to the reporting and flagging of content;

f) Establishing and operating age verification systems for users of VSPS with respect to content which may impair the physical, mental or moral development of minors;

g) Establishing and operating easy-to-use systems allowing users of VSPS to rate content that may impact the physical, mental or moral development of minors;

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;

i) Establishing and operating transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints to the VSPS provider in relation to the implementation of the measures relating to reporting and flagging, age verification, content rating and parental control systems;

j) Providing for effective media literacy measures and tools and raising users' awareness of those measures and tools.

This section of the Call for Inputs focuses on these ten measures. We have grouped the measures into two main categories below: Online Safety Features for Users and then Terms and Conditions, Content Moderation and Complaints. These categories are explored in more detail in sections 5.1 and 5.2. We explore additional measures we might require VSPS providers to take and other important issues (such as regulatory cooperation) in section 5.3.

5.1 Online Safety Features for Users

We anticipate that the Code will require VSPS providers to design and implement online safety features for their users. In this section we are seeking your views on the measures from Article 28b.3 of the AVMSD that focus on online safety features, namely: measures (c), (d), (e), (f), (g), (h) and (j). It would be helpful if you could point us towards existing examples of online safety features that have been designed effectively in your responses to our questions.

Please note that the AVMSD requires that personal data of minors collected or otherwise generated by VSPS providers implementing age-verification systems, content rating systems and parental control systems must not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.

5.1.1 Feature for Declaring Commercial Communications – Measure (c)

In the Code we plan to require VSPS providers to implement a feature for users to declare when the videos they upload contain commercial communications (as far as they know or can be reasonably expected to know). Commercial communications are marketing messages included in, or provided with, content that is designed to directly or indirectly promote the goods, services or image of a person pursing an economic activity. They are included in, or provided with, content in return for payment or for similar consideration or for self-promotional purposes. Advertising, sponsorship and product placement are all examples of commercial communications. In the case of Influencer marketing, this entails companies paying influencers to include commercial communications in the content they upload.

Commercial communications are an important source of funding for content creators and we do not intend the Code to prohibit or inhibit legitimate forms of commercial communications. We would like this feature to clearly let users know when they are being targeted with commercial messages. It will help prevent them from being misled and allow them to judge the merits or otherwise of a product or service featured more effectively. The feature will also help to address surreptitious or misleading commercial communications.

Many social media services have existing mechanisms that allow users to declare whether videos contain ads. Research published last year by Ireland's Competition and Consumer Protection Commission[16] found that labels such as "#workswith[brand]" did not enable users to clearly identify the content as a commercial communication. The CCPC report recommended that a small number of tags such as "#advertisement", "#AD" and "#PaidPartnership" should be used.

[16] *Influencer Marketing* – CCPC, December 2022, https://www.ccpc.ie/business/wp-content/uploads/sites/3/2022/12/2022.12.12-172837-CCPC-Influencer-marketing-report.pdf

In addition to tags applied by uploaders, it would also be possible for VSPS providers to include a meta-data field indicating whether or not a piece of content contained a commercial communication. Use of such a field could enable the VSPS provider to better monitor whether or not the communication complied with other requirements, such as not exploiting children.

> **Question 8: How should we ask VSPS providers to introduce a feature that allows users to declare when videos contain advertising or other type of commercial communications? Should the Code include specific requirements about the form in which the declaration should take? What current examples are there that you regard as best practice?**

5.1.2 Flagging Mechanism – Measures (d) & (e)

We plan to require VSPS providers to establish and operate transparent and user-friendly mechanisms for users to report or flag content in the Code. We also expect to require VSPS providers to establish and operate systems to explain the decisions they make after content has been reviewed.

VSPS vary in terms of their users, size and the kinds of content they make available. What works best as a flagging mechanism may vary from service to service. We are interested in hearing your views about common expectations and standards for how these features should be designed.

The DSA (Article 16) will require platforms to put in place a notification mechanism for illegal content and require them to process the notifications in a timely, diligent, non-arbitrary and objective manner. We are interested in hearing your views on whether it might be possible to integrate the mechanism we ask VSPS providers to introduce in the Code with this mechanism. This might be more convenient for users than having to determine whether they are flagging content under the DSA or the Code.

Please note that this question focuses on the **design** of the flagging mechanism itself (e.g. how it appears on the service's user-interface, the functionality it provides). We address how VSPS providers prioritise and address content moderation issues that have been flagged to them and potential timescales for content moderation decisions in section 5.2.

> **Question 9: How should we ask VSPS providers to introduce and design a flagging mechanism in the Code? How can we ensure that VSPS providers introduce the mechanism in a user-friendly and transparent way? How should we ask VSP Providers to report the decisions they've made on content after it has been flagged? To what extent should we align the Code with similar provisions on flagging in the DSA?**

5.1.3 Age Verification and Age Assurance Features – Measure (f)

We plan to require VSPS providers to introduce appropriate age-verification mechanisms to protect minors from online harms in the Code. Article 28b of the AVMSD requires content that is most harmful to minors to be subject to the strictest access control measures.

Some potentially harmful content is inappropriate for all minors; other content may be suitable for older children but not younger ones. A VSPS provider may need a system for verifying that a user is an adult or is above a certain age depending on the content that is permitted.

There are a range of systems and measures that can be used for age assurance or age verification. These vary in complexity, in the level of confidence in their accuracy and in the extent to which they require acquisition of users' personal data. The simplest form of age assurance is 'age gating' where access to a service will be gained by entering a declared age. Self-declaration has the drawback that minors can easily declare an age that is older than their real age to access a service.

A more sophisticated approach may be to use age-estimation based on artificial intelligence to approximate a sense of a user's age and to compare this with a self-declared age. VSPS providers who use this technique have data on the number of accounts that they have detected that belong to minors who have claimed to be adults. But this data is not conclusive in assessing the effectiveness of age-estimation techniques. Data on the proportion of minors that claim to be adults but evade detection would be more useful but is inherently harder to collect.

More robust age verification involves relying on documents such as a driver's licence or passport, or alternatively biometric data that may be collected via certain services and devices. These techniques involve sharing personal data, though this can be done via third parties so that the VSPS provider is merely informed of the user's verified age group. There is a proposal for a European Digital Identity that would provide EU citizens with a means of proving their age without disclosing any other personal data, but this is not yet in place.

We would like your views on what sort of age verification and age assurance measures you think it would be appropriate for us to ask VSPS providers to take in the Code. We are interested in your views on whether there are high risk categories of content that should be subject to the strictest age verification methods and if there are lower risk categories that may require a lower order of verification or assurance. We are also interested in any views on whether the protection of minors from online harms needs to be balanced against the right or desire of adults to anonymously access certain types of content that is suitable for them but which may not be suitable for children. We are also interested in any evidence about the effectiveness of age estimation techniques.

Finally, we are interested in your views on what sort of content should be shown to users who are not logged in to a service or who are in private browsing mode and whose age cannot be verified or accurately assured. Should such users be shown only content that is deemed suitable for the youngest users?

Question 10: What requirements should the Code include about age verification and age assurance? What sort of content should be shown by default to users who are logged out or in private browsing mode and whose age cannot be verified or assured? What evidence is there about the effectiveness of age estimation techniques? What current practices do you regard as best practice? Where accounts are not age verified should default privacy settings be used, should content default to universal content and should contact by others be more limited?

5.1.4 Content Rating Feature – Measure (g)

We anticipate that the Code will require VSPS providers to establish and operate easy-to-use systems that allow users to age-rate the videos they upload. The type of content ratings systems that people will be familiar with are those that can be found on movies, on television or on-demand services and on video games. We anticipate that effective content rating systems on VSPS will help to make parental control measures and age-verification measures more effective by ensuring that content is appropriately rated at the point where it is uploaded or shared.

Content rating systems empower viewers of content or the parents or guardians of children to decide whether content is suitable. Rating systems generally recognise that children under 18 are not a uniform group and some children of the same age will have differing levels of maturity. Certain content will be more impactful on different children because of their life experience, their personality or their maturity.

The classification frameworks used for movies in different Member States are similar but not identical. For example, the Irish Film Classification Office uses five categories to classify film content (G, PG, 12A, 15A, 16 and 18). A film classified as 'G' is one that should be suitable for children of a school going age while a film classified as '15A' is one deemed appropriate for viewers of fifteen and over. However, they can also be seen by younger children – provided they are accompanied by an adult who has deemed the film appropriate viewing for that child. In Germany, the categories are: suitable for all ages, 6 and up, 12 and up or 6 and up if accompanied, 16 and up, and adults only.

As VSPS content can be viewed throughout the EU, it might be desirable to have a single content rating framework for all VSPS to use. It will be important that the mechanism for users to classify content is actually used and that VSPS providers take steps to help users understand content rating schemes. We also need to consider how VSPS providers should assure the accuracy of content rating.

You should feel free to address issues relating to the design of the content rating mechanism itself and issues relating to the adoption of content rating schemes by users in your response to this question.

> **Question 11: What requirements should the Code have in relation to content rating? What do you consider to be current best practice? What experiences have you had using content rating systems on platforms and do you think they have been effective? What steps could we ask VSPS to take to ensure content is rated accurately by users?**

5.1.5 Parental Controls – Measure (h)

We anticipate that the Code will require VSPS providers to establish and operate appropriate parental control features. Parental controls are systems which allow parents or guardians to filter content viewable to minors or to make choices about how minors experience a service. They can be helpful for parents and guardians to reduce the risks of children being exposed to content that will be detrimental to their physical, moral or mental development.

Different parental controls offer different functionalities and they can vary from service to service. Common features of parental control systems allow parents and guardians to set time limits on a child's use of the service or control or block access to certain age-inappropriate content or to have settings set to private so that strangers cannot contact children.[17] In some instances, parental controls are 'turned-on' by default. This is an example of 'safety by design' and is discussed elsewhere in this Call for Inputs.

Question 12: What requirements should the Code have in relation to parental control features? How can we ensure that VSPS providers introduce the mechanism in a user-friendly and transparent way? Can you point to any existing example of best practice in this area? Should parental controls be 'turned-on' by default for accounts of minors or where age is not verified?

5.1.6 Media Literacy – Measure (j)

Media literacy is defined in the 2009 Act as amended as the public understanding of material published in print, broadcast, online or other media, including the public understanding of – (a) the nature and characteristics of published material; (b) how material is selected, or made available, for publication;(c) how individuals and communities can create and publish material; and (d) how access to published material is or can be regulated. The AVMSD outlines the role of media literacy, which it describes as the skills, knowledge and understanding that allow citizens to use media effectively and safely.

The AVMSD highlights that media literacy is important: to enable citizens to access information and to use, critically assess and create media content responsibly and safely, citizens need to possess advanced media literacy skills. It further states that it is necessary that both media service providers and VSPS providers, in cooperation with all relevant stakeholders, promote the development of media literacy in all sections of society, for citizens of all ages, and for all media, and that progress in that regard is followed closely.

We expect that the Code will ensure that VSPS provide for effective media literacy measures and tools and that they raise users' awareness of those measures and tools. Media literacy measures and tools are important to ensure that users of VSPS understand the features, systems and procedures put in place by VSPS providers to protect citizens from online harms.

Question 13: What requirements should the Code contain to ensure that VSPS provide for effective media literacy measures and tools?

5.2 Terms and Conditions, Content Moderation and Complaints

This section of the Call for Inputs focuses on the Article 28b.3 measures of the AVMSD that require VSPS providers to determine what content is allowed on their services through their terms and conditions and to receive, process, prioritise and make decisions about content issues and complaints raised by users. These are measures (a), (b) and (i) described above in section 5.

[17] This webpage from Webwise provides a good overview of parental control mechanisms that can be utilised - Online safety - How to set up parental controls (webwise.ie).

Content moderation decisions made by VSPS providers can result in a range of actions, including removing or deprioritising content, requiring changes to the content, suspending or terminating accounts or restricting a user's ability to monetise content they have uploaded.

5.2.1 Terms and Conditions (Contents) – Measures (a) and (b)

VSPS providers normally use their terms and conditions as the contractual basis for the content moderation decisions they make and for their content policies. Some VSPS providers choose to have more restrictive rules for content than others – for instance, many VSPS do not permit pornographic content but some do, and some focus on it. We are interested to hear what measures you think we should ask VSPS providers to take in the Code to ensure their terms and conditions adequately protect against online harms. Some possibilities include:

- a prohibition on certain types of harmful content such as incitements to violence or hatred, or content which constitutes a criminal offence;
- a requirement that commercial content, including commercial content uploaded by influencers, must be declared through the service's mechanism for declaring commercial communications and tagged in a particular way;
- a prohibition on commercial content that uses subliminal techniques, promotes tobacco, exploits minors etc;
- if the VSPS provider chooses to allow content which may be harmful to some minors, requiring uploaders to age-rate content, so that the VSPS provider is better able to ensure that unsuitable content is not seen by users who are too young;
- sufficient sanctions for users who break these rules, including account suspension or termination, downgrading their content in recommender systems.

In addition to views about the content of terms and conditions, we are interested in any views about how they are brought to the attention of users – for instance whether there should be a plain language summary, and whether users should be periodically reminded of key terms and conditions.

> **Question 14: How should we ask VSPS providers to address online harms in their terms and conditions in the Code, including the harms addressed under Article 28b? How should key aspects of terms and conditions be brought to users' attention? What examples are there of best practice in relation to terms and conditions including content moderation policies and guidelines?**

5.2.2 Applying Terms and Conditions (Content moderation decisions) – Measures (a) & (b)

VSPS providers' content policies and community guidelines set out the behaviours and content they prohibit and derive from their services' terms and conditions. However, content policies and guidelines will not reduce online harms unless services apply them in practice.

We are seeking your views on how we should ask VSPS providers to make content moderation decisions when they apply the terms and conditions and content policies they have introduced (or amended) to comply with the Code.

We are aware of a number of reasons why content moderation decisions may sometimes be inaccurate or contestable. These include:

- Content moderators may not always be fully aware of the cultural context of the content they are scrutinising. This will result in them sometimes making misjudgements about particular pieces of content.

- Content alleged to be in breach of terms and conditions may pose some risk of harm or be highly offensive but this may not amount be a clearcut breach of VSPS terms and conditions. In these cases the provider must decide whether to err on the side of removing the content or permitting it to remain.

- In cases of cyberbullying, the bullying may involve content on several different platforms as well as offline activity. A provider who is aware only of one piece of content on its own platform may not recognise it as cyberbullying.

We are interested in views about whether there should be requirements in the Code about the accuracy of moderation decisions. In particular, we are interested in hearing about how we should ask platforms to measure the accuracy of the decisions they make and how they should balance this with the need to make decisions quickly. What challenges have platforms faced with this issue in practice and what difficulties have they experienced where there are grey areas?

We are also interested in hearing views about whether the Code should set out requirements and standards in the content moderation process. For instance, should there be a process in all cases for moderators to refer borderline cases for a second opinion?

We are interested to hear about the resource implications of different approaches to making moderation decisions and how you think services should prioritise the different kinds of decisions they have to make (we discuss automated decision-making below). Do you think services should be mandated to prioritise requests from certain bodies e.g. other regulators?

We are also interested in views about the measures we could ask VSPS providers to take where they find content breaches their terms and conditions and what different factors they should consider when they make these decisions. For instance, high-risk content that was clearly in breach might result in immediate account suspension or termination, whereas medium-risk content that was not clearly in breach might be placed behind a content warning or deprioritised in recommender systems. In particular, we are interested in whether you think we should specify timescales by which decisions must be taken and what information should be provided to the user or body that has flagged allegedly harmful content.

We are also interested in hearing your views on whether we should take a different approach in the Code to regulating how VSPS providers make decisions about illegal content.

We are aware that many platforms have implemented mechanisms to automatically detect and/or moderate content. Platforms have told us that the bulk of their decisions to remove content results from automated flagging rather than user notifications. They also say that content flagged by users is less likely to be found to be in breach of content rules than automatically flagged content. They say this occurs in part because of the volume of complaints that are made about items that do not infringe content rules or in some cases are made even in bad faith.

Automated content detection and moderation mechanisms can make a very important contribution to online safety by managing content at scale more effectively than human moderation. But these systems may make mistakes and this can result in user-flagged content being de-prioritised for review by moderators. This may be an appropriate or inappropriate response based on the content flagged and raises potential questions about balancing rights to expression with protection from harm.

We are aware the most acute distress can occur when a platform does not act swiftly to review a notification by the user. We are interested in views about what an Online Safety Code might do to encourage the use of effective automated detection and moderation tools, while also ensuring that genuine notifications from users are processed quickly and that errors these systems make are addressed appropriately.

Imposing a general monitoring obligation on VSPS providers would conflict with the E-Commerce Directive. However, targeted and proportionate obligations to monitor particular categories of content are not precluded.

The DSA (Article 22) also requires platforms to give priority to notices about illegal content from "trusted flaggers" who have been awarded this status in any Member State. We would be interested in views on whether the Code should extend this to notices about alleged breaches of VSPS content rules. This might be more convenient for users, for trusted flaggers and for VSPS providers than establishing a parallel system of trusted flaggers in the Code or for nominated bodies under the 2009 Act as amended.

> **Question 15: How should we ask VSPS providers to address content moderation in the Code? Are there any current practices which you consider to be best practice? How should we address automated content detection and moderation in the Code?**

5.2.3 Complaint Handling – Measure (i)

A complaint occurs when a user expresses dissatisfaction with the way a VSPS provider has acted. This is separate from a user requesting a VSPS provider to remove a piece of content that they consider to be harmful.

Examples of complaints could be:

- A user is dissatisfied with a content moderation decision;
- A user is dissatisfied that they did not receive a response to a notice about alleged harmful content within the required timescale;

- An uploader is pressured into agreeing with a content removal or restriction decision because their account will remain restricted for a lengthy period if they appeal;
- A parent or guardian considers that a VSPS provider has shown their child content that was not appropriate for their age;
- A parent or guardian finds that a VSPS provider has implemented its parental control system in a confusing way;
- A user considers that the service's rules for content rating are not appropriate.

We anticipate that the Code will (a) require VSPS providers to establish and operate transparent, easy-to-use and effective procedures for handling users' complaints; and (b) require VSPS providers to report to the Commission at intervals, specified in the Code, of not more than 3 months on the provider's handling of communications from users raising complaints and other matters.

We are interested in views on what channels VSPS providers should be required to make available to receive complaints, what timescales there should be for acknowledging and responding to complaints, and how users should be made aware of complaint-handling procedures. We are also interested in hearing from you about how you think VSPS providers should prioritise the complaints they receive.

The DSA (Article 20) provides that platforms must operate an internal complaint-handling system in relation to content moderation decisions, which will cover at least some of the issues that could lead to complaints arising under the Code. We are interested in views as to whether the Code should require VSPS providers to operate an integrated complaint-handling system covering both DSA and Online Safety Code matters. This might be convenient both for users and VSPS providers.

The DSA (Article 21) provides that complainants may select a certified out-of-court dispute resolution body to resolve a dispute if they are not satisfied with the response from a provider's internal complaint handling process. We are interested in views as to whether complainants should be able to use the same dispute resolution bodies to resolve disputes that concern the Code as well as the DSA – recognising that some complaints or disputes might arise under both instruments.

Please note that we are not seeking views at this time on how the Commission itself should deal with individual complaints. This will be the subject of a later consultation process.

> **Question 16: What requirements should the Code include about procedures for complaint-handling and resolution, including out-of-court redress or alternative-dispute resolution processes? To what extent should these requirements align with similar requirements in the DSA? What current practices could be regarded as best practice? How frequently should VSPS providers be obliged to report to the Commission on their complaint handling systems and what should those reports contain? Should there be a maximum time-period for VSPS providers to handle user complaints and if so, what should that period be?**

5.3 Possible Additional Measures and Other Matters

This section covers additional measures that we may expect VSPS providers to take under the Code, such as following a "safety by design" approach when they introduce new features. We also explore other important matters such as regulatory cooperation.

5.3.1 Accessible Online Safety Features

We anticipate that the Code will require VSPS providers to ensure the online safety features they introduce are transparent, user-friendly and easy to find. We would be interested in hearing your views about what steps you think we could ask VSPS providers to take to ensure these features and other measures taken under the Code (e.g. receiving complaints) are accessible to users with disabilities.

Question 17: What approach do you think the Code should take to ensuring that the safety measures we ask VSPS providers to take are accessible to people with disabilities?

5.3.2 Risk assessments

The DSA (Articles 34 and 35) will require VSPS that have been designated as Very Large Online Platforms (VLOPs) to prepare systemic risk assessments and to implement risk mitigation measures. There is an alignment between the topics that must be covered in these risk assessments and the risks of harm to be addressed by the Code. We are interested in hearing whether the Code should require providers of services that are designated both as a VSPS provider and as a VLOP to carry out a similar assessment of the risk of the dissemination of harmful content of the type covered by the Code. The assessment could be integrated with the risk assessment required by the DSA if the provider so wished.

Alternatively, we could require a more bespoke assessment of the availability of harmful online content, the risk of it being available and of the risk posed to users. This could also include a children's rights impact assessment. Risk assessments could help platforms determine, and provide an objective basis for justifying, the measures they have taken to comply with the Code.

5.3.3 Safety by design

Safety by design involves identifying safety risks in advance of developing a new product or service and considering how to mitigate those risks. The fact that motor vehicles have seat belts and airbags as an automatic part of the vehicle design is an example of safety by design.[18]

One approach to reflecting this in the Code would be to require VSPS providers to publish a "Safety by Design" statement setting out how they consider online safety when developing or enhancing services. We could include a requirement to prepare a "Safety Impact Assessment" whenever services are being developed or enhanced, with sign-off of the risk assessment and proposed mitigation measures by an executive staff member of the VSPS provider with appropriate experience and responsibilities.

[18] See here for more information on Safety by Design - https://www.esafety.gov.au/industry/safety-by-design and here - 5Rights | Design of Service (5rightsfoundation.com)

We are interested in views about this approach – or other possible approaches – to reflecting safety by design in the Code.

Question 18: What approach do you think the Code should take to risk assessments and safety by design? Are there any examples you can point us towards which you consider to be best practice?

5.3.4 Cooperation with other Regulators, Bodies

The Code has to ensure that VSPS providers take appropriate measures to protect their users across Europe. Some of Europe's largest VSPS providers are based in Ireland and they provide large quantities of content to users in different languages and locations across the continent.

The Commission already cooperates with other statutory regulators. We belong to the European Regulators Group for Audiovisual Media Services (ERGA). Over the years ERGA Members have worked together to improve cross-border cooperation on media regulation matters and in 2021 agreed a Memorandum of Understanding to strengthen cooperation further. The Commission is also a member of the Global Online Safety Regulators Network. Finally we will be a digital services coordinator under the DSA working closely with digital services coordinators throughout the EU and with the European Commission. Within Ireland we are part of the Digital Regulators Group working closely with the Data Protection Commission (DPC), Commission for Communications Regulation (ComReg) and the Competition and Consumer Protection Commission (CCPC).

Question 19: How do you think that cooperation with other regulators and bodies can help us to implement the Code for VSPS?

5.3.5 Harmful feeds and recommender systems

Some civil society groups have highlighted instances where severe harm has been caused by the aggregate of content viewed by a vulnerable person, even though many of the individual pieces of content might not have been harmful if viewed in isolation.

The algorithms used by recommender systems to create a feed of content can be designed to mitigate this risk – for instance by ensuring that the feed contains a mix of different types of content and does not come to be dominated by, say, content related to beauty and fitness. A feed which contains too much content of this type may increase the vulnerability of a user to eating or feeding disorders. Likewise, a feed that is dominated by negative or depressing content may gravely impact mental health leading to the risk of self-harm or in serious cases suicide.

We are interested in hearing whether you think the Code should require VSPS providers to ensure their recommender systems do not result in a feed of content which in aggregate risks causing harm. We would also be interested in whether there are particular practices that the Code could mandate in this regard such as safety by design or otherwise including intercepting a negative feed with positive content.

Question 20: What approach do you think we should take in the Code to address feeds which cause harm because of the aggregate impact of the content they provide access to? Are there current practices which you consider to be best practice in this regard?

5.3.6 Audiovisual commercial communications arranged by the VSPS provider

Many VSPS providers directly market, sell and arrange commercial communications that are viewed by their users. An example might be a video ad that a viewer sees before they can view an uploaded video. The Code has to ensure that where a VSPS provider is responsible for marketing, selling or arranging commercial communications that these comply with advertising standards requirements from the AVMSD.

> **Question 21: Do you have any views on how requirements for commercial content arranged by a VSPS provider itself should be reflected in the Code?**

5.3.7 Compliance

We are responsible for assessing the appropriateness of the measures that VSPS providers take under Article 28b.5 of the AVMSD. This is an important provision of the AVMSD that is designed to ensure VSPS providers comply with national laws and regulatory measures transposing Article 28b in practice.

For us to carry out our assessments we expect we will need VSPS providers to create and share information about the risks posed by their services with us and to explain the decisions they have made about how to comply with the Code.

The risk of harm on a service will, among other things, inform the measures it must take.[19] For example, if a service has lots of users who are children, then how the service approaches protecting minors may be a greater concern for us. Conversely, if a service has effective age-verification in place or has verified it has a very low number of users who are children then taking appropriate measures in other areas may be more of a focus for the service.

We also need to consider how and when VSPS providers report to us about how they have complied with the Code. We can require they report to us in a structured way in the Code and we can also require providers to provide us with information about their compliance with the Code on an ad hoc basis. We would welcome views on whether we should require an annual compliance statement, approved by the Board of Directors of a VSPS provider. This would ensure that compliance and the internal governance arrangements that assure it are matters that get attention at an appropriately senior level.

Finally, we also need to consider how we should approach things if a service's conduct falls short of that expected by the Code. We will develop an overall compliance and enforcement approach to VSPS at a later time but welcome any views you have on this issue now.

[19] Article 28b.3 provides that the measures taken by VSPS 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. It also provides that 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, and that 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.

Question 22: What compliance monitoring and reporting arrangements should we include in the Code?

5.3.8 Transitional Arrangements

New regulatory instruments often have "transition periods" before they fully come into effect. These give regulated entities time to prepare for new regulatory arrangements. We anticipate including a transition period in the Code to give VSPS providers time to adapt to the requirements. At the same time, we would not want transitional arrangements to lead to unnecessary compliance delays where services have the means to comply with the Code sooner. Transitional arrangements could apply to the entire Code or to specific provisions of it where appropriate.

Question 23: Should the Code have a transition period or transition periods for specific issues? Which areas touched on in this Call for Inputs may VSPS providers require time to transition the most? What time frame would be reasonable for a transition period?

6. Data Protection and Freedom of Information

Use of Information

The Commission shall comply with its obligations under the General Data Protection Regulation ("GDPR"), the Data Protection Act 2018 and any other applicable data privacy laws and regulations. The Commission is obligated and committed to protecting all personal data submitted. The Commission has an appointed a Data Protection Officer who is registered with the Data Protection Commission. Respondents can find out more on how the Commission processes personal information in the Commission's published policy at: https://www.bai.ie/en/about-us/data-protection-policy/

For this process, the Commission will collect the name, email address and any other personal information that is included in your response. The name of the respondent to the Call for Inputs and the response provided will be made publicly available. However, the Commission will not make publicly available your contact details, such as your address, phone number or email.

The information collected will be used only for the purposes of this Call for Inputs and for no other purpose. Please clearly mark any information that you consider to be confidential in your response.

Confidential Information

It is the Commission's intention to publish submissions received in response to this Call for Inputs. Please provide your response as a non-confidential document, with confidential information contained in a separate annex, or submit a redacted non-confidential version together with your response.

Freedom of Information

Information held by the Commission is subject to its obligations under law, including under the Freedom of Information Act 2014. The Commission will consult with you about any information you mark as confidential before making a decision on any Freedom of Information request received.

Coimisiún na Meán

Annex 1

Information for Organisations Representing Children and Young People

Coimisiún na Meán and the Online Safety Code

Coimisiún na Meán ("the Commission") is Ireland's new media commission for regulating broadcasters, video on-demand and online safety. One of the main jobs that the Commission must undertake is developing an Online Safety Code. This Code will apply to video-sharing platforms. These are online platforms that allow people, including children and young people, to share and view video content on the internet. These videos can be watched using websites or apps. The purpose of the Code is to help protect and keep safe from harm anyone, but particularly children and young people, watching video content on websites or apps. It will not cover private messaging. We have developed this annex to assist groups representing children and young people to engage with them on the Online Safety Code.

Developing the Online Safety Code

An important part of the process that the Commission will undertake to develop the Code is gathering the views of people about how the Code should protect users of video-sharing platforms. The opinions of children and young people are an important part of this process and there are a number of ways that the Commission plans to communicate with them and their representatives about this new Online Safety Code. This will include gathering input over three stages.

- Firstly, the Commission is asking the public, video-sharing platforms, and anyone who is interested in online safety to tell us how the Code being development by the Commission can keep users safe from harm. This first stage is called the 'Call for Inputs' stage. This annex to the Call for Inputs has been developed as part of this stage to assist groups and organisations to engage with children and young people that they represent on the development of the Code.

- Secondly, the Commission will consider the responses to the Call for Inputs and all other relevant information gathered as part of this process, including research. It will then write a draft version of the Online Safety Code. The Commission will then publish this draft Code and ask for views on this draft. This stage will be called the 'Public Consultation' stage. As part of this stage, the Commission intends to undertake a more extensive engagement with children and young people.

- Thirdly, the Commission intends to establish a new Youth Advisory Committee. Half of the members of the Committee will be people over the age of 25 who work with child and youth organisations and the other half will be people aged under the age of 25. This Committee will be asked by the Commission to tell us what they think of the draft Online Safety Code.

Call for Inputs – How you can help?

We are inviting organisations representing children and young people under the age of 25 to ask, where practicable, their members, including youth panels and youth committees, about the issues raised in our Call for Inputs. We have drafted several questions below that children and youth-focused groups and organisations may find useful for this.

These questions are indicative and you should feel free to tailor them to those that you represent or work with. We would be grateful if responses could be submitted together with your main response.

Indicative Questions – Questions are about video-sharing platforms only.

Q1. What do you like about being able to watch or share videos on websites or apps?

Q2. How safe do you feel when you are watching or sharing videos on websites or apps?

Q3. Are you concerned about any videos that you see on websites or on apps? If you are, what types of videos concern you the most?

Q4. Do you feel that you have enough control over the type of videos that you see on websites or apps?

Q5. Do you think that companies who run websites or apps that allow videos to be watched or shared should do anything to make things safer for you or your friends or family?

Q6. How old do you think a child should be before they should be allowed to watch or share videos on websites or in apps? Should there be different rules for children who are different ages?

Q7. Have you ever reported your concerns to your parent/s or guardian/s or to a company in charge of websites or apps about a video that you have seen? How did that go?

Q8. Is there anything else you would like to comment on?

Appendix 1

Legislative Provisions

Online Safety and Media Regulation Act 2022 – Part 11: Online Safety

Harmful online content

139A.— (1) For the purposes of this Act, online content is 'harmful online content' if it is one of the following 2 kinds:

(a) content that falls within one of the offence specific categories of online content defined in subsection (2);

(b) content that –

(i) falls within one of the other categories of online content defined in subsection (3), and

(ii) meets the risk test defined in subsection (4).

(2) The offence-specific categories of online content are –

(a) the categories listed in Schedule 3, and

(b) any category specified for the purposes of this paragraph by order under section 139B.

(3) The other categories of online content are:

(a) online content by which a person bullies or humiliates another person;

(b) online content by which a person promotes or encourages behaviour that characterises a feeding or eating disorder;

(c) online content by which a person promotes or encourages self-harm or suicide;

(d) online content by which a person makes available knowledge of methods of self-harm or suicide;

(e) any category specified for the purposes of this paragraph by order under section 139B.

(4) Online content meets the risk test for the purposes of subsection (1)(b) (ii) if it gives rise to –

(a) any risk to a person's life, or

(b) a risk of significant harm to a person's physical or mental health, where the harm is reasonably foreseeable.

(5) For the purposes of this Act, any question whether particular online content falls within a category under this section shall be determined on the balance of probabilities.

Power to specify other harmful online content

139B. — (1) If the Commission makes a proposal to the Minister that a category of online content should be specified for the purposes of section 139A(2)(b) or (3)(e), the Minister may make an order giving effect to the proposal.

(2) Section 139C sets out the procedure for proposals and orders under subsection (1).

(3) A proposal under subsection (1) that a category of online content should be specified for the purposes of section 139A(2)(b), and an order giving effect to such a proposal, may be made only if –

(a) it is a category of content by which a person does a thing contrary to an enactment specified in the proposal, and

(b) the thing done is an offence under that enactment.

(4) The Commission may make a proposal under subsection (1) only if satisfied –

(a) that giving effect to the proposal will enable the Commission to take action against significant risks posed by the content within the proposed category,

(b) that those risks are not sufficiently addressed by available means (including means available to other regulators, providers of relevant online services, or others), and

(c) that, having regard to the protection of children, to the protection of the public generally, and to all other relevant considerations, it is in the public interest to give effect to the proposal.

(5) In deciding whether to make a proposal under subsection (1), the Commission shall have regard in particular to –

(a) levels of availability of any online content on relevant online services,

(b) levels of risk of exposure to any online content when using relevant online services,

(c) levels of risk of harm, and in particular harm to children, from the availability of content or exposure to it,

(d) changes in the nature of online content and in levels of availability and risk referred to in paragraphs (a) to (c),

(e) the impact of automated decision-making in relation to content delivery and content moderation by relevant online services, and

(f) the rights of providers of designated online services and of users of those services.

Procedure for proposals and orders under section 139B

139C. — (1) The Commission may make a proposal under section 139B(1) only if—

(a) the Commission has published a draft of the proposal in a way that it thinks appropriate to bring it to the attention of members of the public,

(b) it has published with the draft a notice stating how members of the public may submit comments to it, and within what time,

(c) it has consulted about the draft any advisory committee it has established for that purpose under section 19,

(d) it has carried out any other consultation that it considers appropriate on the draft, and

(e) it has considered any comments submitted to it in accordance with a notice under paragraph (b) or in consultation under this subsection.

(2) On receiving a proposal the Minister shall—

(a) consult the Joint Oireachtas Committee,

(b) consider the proposal in the light of that consultation and any other consultation the Minister considers appropriate, and

(c) respond to the Commission within a reasonable time.

(3) The Minister's response must be either—

(a) to accept the proposal for consideration by the Government, or

(b) to request the Commission to reconsider the proposal.

(4) The Minister may make an order under section 139B(1) giving effect to a proposal only if—

(a) the Minister has accepted the proposal for consideration by the Government, and

(b) the Government has approved the proposal.

(5) The Minister may accept a proposal for consideration, and the Government may approve a proposal, only if satisfied of the matters listed in section 139B(4).

(6) In deciding whether to accept or approve a proposal, the Minister and the Government shall have regard in particular to the matters listed in section 139B(5).

(7) Where an order is proposed to be made under section 139B(1), a draft of the order shall be laid by the Minister before each House of the Oireachtas and the order shall not be made unless a resolution approving the draft has been passed by each such House.

Age-inappropriate online content

139D. — In this Part, 'age-inappropriate online content' means online content that is likely to be unsuitable for children (either generally or below a particular age), having regard to their capabilities, their development, and their rights and interests, including in particular content consisting of—

(a) pornography, or

(b) realistic representations of, or of the effects of, gross or gratuitous violence or acts of cruelty.

Online safety codes

139K. — (1) The Commission may make codes ('online safety codes'), to be applied to designated online services in accordance with section 139L.

(2) An online safety code may make provision with a view to ensuring—

(a) that service providers take appropriate measures to minimise the availability of harmful online content and risks arising from the availability of and exposure to such content,

(b) that service providers take any other measures that are appropriate to protect users of their services from harmful online content,

(c) that service providers take any other measures that are appropriate to provide the protections set out in Article 28b(1)(a), (b) and (c) of the Directive, and

(d) that service providers take any measures in relation to commercial communications on their services that are appropriate to protect the interests of users of their services, and in particular the interests of children.

(3) In the case of video-sharing platform services, the Commission shall exercise its powers under this section with a view to ensuring (without prejudice to any other exercise of those powers in relation to video-sharing platform services) that service providers—

(a) take appropriate measures to provide the protections referred to in subsection (2)(c), including appropriate measures referred to in Article 28b(3) of the Directive,

(b) comply with the requirements set out in Article 9(1) of the Directive with respect to audiovisual commercial communications that are marketed, sold or arranged by them, and

(c) take appropriate measures to comply with the requirements set out in Article 9(1) of the Directive with respect to audiovisual commercial communications that are not marketed, sold or arranged by them, taking into account the limited control they exercise over those communications.

(4) Without prejudice to subsection (2) an online safety code may provide for:

(a) standards that services must meet, practices that service providers must follow, or measures that service providers must take;

(b) in particular, standards, practices or measures relating to the moderation of content or to how content is delivered on services;

(c) the assessment by service providers of the availability of harmful online content on services, of the risk of it being available, and of the risk posed to users by harmful online content;

(d) the making of reports by service providers to the Commission;

(e) the handling by service providers of communications from users raising complaints or other matters.

(5) Without prejudice to subsection (2) or (4), an online safety code may prohibit or restrict, in accordance with law, the inclusion in programmes or user-generated content of commercial communications relating to foods or beverages considered by the Commission to be the subject of public concern in respect of the general public health interests of children, in particular infant formula, follow-on formula or foods or beverages which contain fat, trans-fatty acids, salts or sugars.

(6) Without prejudice to subsection (4), the Commission shall make an online safety code, to be applied in accordance with section 139L to such designated online services as the Commission considers appropriate, requiring the service provider to report to the Commission at intervals, specified in the code, of not more than 3 months on the provider's handling of communications from users raising complaints or other matters.

(7) In this section, 'service provider' means the provider of a designated online service.

Application of online safety codes

139L. — (1) An online safety code applies to a designated online service if—

(a) the Commission has determined that the code is to apply to the service, or to a designated category of services that includes the service,

(b) the Commission has given notice of the determination, and the notice has taken effect, in accordance with subsection (2), and

(c) the determination has not been revoked.

(2) Notice under subsection (1)(b)—

(a) in the case of a service designated as a named service, must be given to the provider of the service in writing, and takes effect when the notice is given to the provider, and

(b) in the case of a designated category of services, must be given by publication of notice of the determination on a website maintained by the Commission, and takes effect at the end of the period of 28 days after the date on which the notice is published on the website.

(3) Before making or revoking a determination under subsection (1) in relation to a named service or a category of services, the Commission shall have regard in particular to —

(a) the nature and the scale of the service, or of services within the category,

(b) levels of availability of harmful online content on the service, or on services within the category,

(c) levels of risk of exposure to harmful online content when using the service, or services within the category,

(d) levels of risk of harm, and in particular harm to children, from the availability of harmful online content or exposure to it on the service, or on services within the category,

(e) the rights of the provider of the service, or providers of services within the category, and

(f) the rights of users of the service, or users of services within the category.

(4) Before making or revoking a determination under subsection (1), the Commission shall consult—

(a) where the designation is of a named service, the provider of the service,

(b) where the designation is of a category of services—

(i) an organisation representative of providers of services falling within the category, if there is such an organisation, and

(ii) the providers of those services, so far as the Commission is able to consult them,

(c) any advisory committee the Commission has established for that purpose under section 19, and

(d) any other person the Commission considers appropriate.

(5) An online safety code applying to an interpersonal communications service or a private online storage service applies to that service only in so far as it relates to content that falls within one of the offence-specific categories of online content defined in section 139A(2).

(6) In this section—

'interpersonal communications service' means a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information between a finite number of persons by means of electronic communications networks, where the persons initiating or participating in the communication determine its recipients, but it does not include services which enable interpersonal and interactive communication only as a minor ancillary feature that is intrinsically linked to another service;

'private online storage service' means any service providing online storage, other than—

(a) local or temporary storage, or

(b) storage provided for the purpose of enabling the provision of another service, or as a minor ancillary feature intrinsically linked to another service;

'temporary storage' means the automatic, intermediate and temporary storage of information for the sole purpose of making more efficient onward transmission of that information.

Online safety codes: matters to be considered

139M. — When preparing an online safety code the Commission shall have regard in particular to—

(a) the desirability of services having transparent decision-making processes in relation to content delivery and content moderation,

(b) the impact of automated decision-making on those processes,

(c) the need for any provision to be proportionate having regard to the nature and the scale of the services to which a code applies,

(d) levels of availability of harmful online content on designated online services,

(e) levels of risk of exposure to harmful online content when using designated online services,
(f) levels of risk of harm, and in particular harm to children, from the availability of harmful online content or exposure to it,

(g) the rights of providers of designated online services and of users of those services, and

(h) the e-Commerce compliance strategy prepared under section 139ZF.

Online safety codes: procedure

139N. — (1) Before making an online safety code, the Commission—

(a) shall consult—

(i) any advisory committee it has established for that purpose under section 19, and

(ii) any other person the Commission thinks appropriate,

And

(b) may consult a public health authority about any provision of an online safety code referred to in section 139K(2)(d) which it proposes to make.

(2) As soon as practicable after making an online safety code, the Commission shall give a copy of the code to the Minister.

(3) As soon as practicable after receiving a copy of an online safety code under subsection (2), the Minister shall lay copies of the code before each House of the Oireachtas.

(4) The Commission may at any time amend or revoke an online safety code, or any provision of an online safety code, and subsections (1) to (3) apply to an amendment or revocation of an online safety code as they apply to an online safety code.

(5) The Commission shall from time to time review the operation of any online safety code it makes.

(6) If the Minister makes a request in writing to the Commission to review the operation of an online safety code, the Commission shall carry out the review and give the Minister a report on the review in writing within a reasonable time.

(7) The Commission shall publish a report given to the Minister under subsection (6) on a website maintained by the Commission.

Compliance with online safety codes: information notices

139O. — (1) The Commission may by notice in writing require the provider of a designated online service to provide the Commission with information relating to the provider's compliance with an online safety code over any period, and may require such information to be provided periodically for a succession of periods.

(2) A notice must—

(a) identify the information to be provided and the period or periods it must relate to, and

(b) state when the information is to be provided.

(3) A notice may not require information to be provided before the end of the period of 7 days beginning on the date on which the notice is received by the provider.

(4) The Commission may at any time by notice in writing extend the time within which information is to be provided.

(5) If within the period referred to in subsection (3) the provider requests the Commission to make an extension under subsection (4), the period beginning with the date on which the Commission receives the request and ending on the date notice of the Commission's decision on the request is received by the provider does not count towards the time within which the information is to be provided.

(6) The provider of a designated online service is guilty of a category 1 offence if—

(a) the provider fails without reasonable excuse to comply with a notice under subsection (1), or

(b) in purported compliance with a notice under subsection (1), the provider provides false information, knowing that it is false or being reckless as to whether it is false.

(7) If the Commission is notified by a nominated body of a matter that appears to the Commission to be relevant to a provider's compliance with an online safety code, the Commission shall consider that matter for the purpose of deciding whether to exercise its functions under this section.

Audit of complaints and complaint handling

139P. — (1) The Commission may appoint a person to carry out an audit under this section, and may by notice in writing require the provider of a designated online service to co-operate with any person appointed.

(2) A notice under subsection (1) may relate to audits to be undertaken periodically, at intervals specified in the notice.

(3) The purpose of an audit under this section is—

(a) to enable the Commission to assess compliance by the provider with provisions of an online safety code that relate to the handling of communications by which users raise complaints or other matters relating to designated online services with the providers of those services, and

(b) to provide the Commission with information to identify any trends in complaints or other matters raised by such communications that may be relevant to the Commission's functions under this Part.

(4) A person appointed to carry out an audit under this section—

(a) must be independent of the provider, and

(b) must not be a Commissioner, or a member of the staff of the Commission.

(5) A notice under this section must—

(a) identify the person appointed to carry out the audit,

(b) identify the provisions of the online safety code that the audit is to assess compliance with,

(c) state when the audit is to commence,

(d) specify the co-operation that may be requested by the person appointed, and

(e) require the provider to provide that co-operation, subject to reasonable notice being given by the person appointed.

(6) The co-operation that may be specified under subsection (5)(d) may include the taking, on reasonable notice from the person carrying out the audit, of steps specified by that person that are reasonably required to assist the carrying out of an audit under this section.

(7) A person who carries out an audit under this section shall provide the Commission with a report on the audit, setting out any information relevant to an assessment in accordance with subsection (3)(a), and any information relevant for the purposes of subsection (3)(b).

(8) The Commission shall provide a copy of the report—

(a) to the provider concerned, and

(b) to the Minister,

and shall give the provider an opportunity to make representations in writing to the Commission on the report within such period as the Commission specifies.

(9) After considering any representations made under subsection (8), the Commission shall publish the report on a website maintained by it, with any redactions the Commission considers necessary on grounds of the personal, confidential or commercially sensitive nature of any part of the report.

(10) If the Commission is notified by a nominated body of a matter that appears to the Commission to be relevant to compliance by a provider with a provision of the kind mentioned in subsection (3)(a), the Commission shall consider that matter for the purpose of deciding whether to exercise its functions under this section.

(11) A provider who fails without reasonable excuse to comply with a notice under subsection (1) shall be guilty of a category 1 offence.

Enforcement of online safety codes

139Q. — A failure by a provider of a designated online service to comply with an online safety code that applies to the service shall be a contravention for the purposes of Part 8B.

Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 - Audiovisual Media Services Directive

Article 28b

1. Without prejudice to Articles 12 to 15 of Directive 2000/31/EC, Member States shall ensure that video-sharing platform providers under their jurisdiction take appropriate measures to protect:

(a) minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development in accordance with Article 6a(1);

(b) the general public from programmes, user-generated videos and audiovisual commercial communications containing incitement to violence or hatred directed against a group of persons or a member of … a group based on any of the grounds referred to in Article 21 of the Charter;

(c) the general public from programmes, user-generated videos and audiovisual commercial communications containing content the dissemination of which constitutes an activity which is a criminal offence under Union law, namely public provocation to commit a terrorist offence as set out in Article 5 of Directive (EU) 2017/541, offences concerning child pornography as set out in Article 5(4) of Directive 2011/93/EU of the European Parliament and of the Council1 and offences concerning racism and xenophobia as set out in Article 1 of Framework Decision 2008/913/JHA.

2. Member States shall ensure that video-sharing platform providers under their jurisdiction comply with the requirements set out in Article 9(1) with respect to audiovisual commercial communications that are marketed, sold or arranged by those video-sharing platform providers.

Member States shall ensure that the video-sharing platform providers under their jurisdiction take appropriate measures to comply with the requirements set out in Article 9(1) with respect to audiovisual commercial communications that are not marketed, sold or arranged by those video-sharing platform providers, taking into account the limited control exercised by those video-sharing platforms over those audiovisual commercial communications.

Member States shall ensure that video-sharing platform providers clearly inform users where programmes and user-generated videos contain audiovisual commercial communications, provided that such communications are declared under point (c) of the third subparagraph of paragraph 3 or the provider has knowledge of that fact. Member States shall encourage the use of co-regulation and the fostering of self-regulation through codes of conduct as provided for in Article 4a(1) aiming at effectively reducing the exposure of children to audiovisual commercial communications for foods and beverages containing nutrients and substances with a nutritional or physiological effect, in particular fat, trans-fatty acids, salt or sodium and sugars, of which excessive intakes in the overall diet are not recommended. Those codes shall aim to provide that such audiovisual commercial communications do not emphasise the positive quality of the nutritional aspects of such foods and beverages.

3. 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.

Those measures shall consist of, as appropriate:

(a) including and applying in the terms and conditions of the video-sharing platform services the requirements referred to in paragraph 1;

(b) including and applying in the terms and conditions of the video-sharing platform services the requirements set out in Article 9(1) for audiovisual commercial communications that are not marketed, sold or arranged by the video-sharing platform providers;

(c) having a functionality for users who upload user-generated videos to declare whether such videos contain audiovisual commercial communications as far as they know or can be reasonably expected to know;

(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;

(e) establishing and operating systems through which video-sharing platform providers explain to users of video-sharing platforms what effect has been given to the reporting and flagging referred to in point (d);

(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;

(g) establishing and operating easy-to-use systems allowing users of video-sharing platforms to rate the content referred to in paragraph 1;

(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;

(i) establishing and operating transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints to the video-sharing platform provider in relation to the implementation of the measures referred to in points (d) to (h);

(j) providing for effective media literacy measures and tools and raising users' awareness of those measures and tools.

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.

4. For the purposes of the implementation of the measures referred to in paragraphs 1 and 3 of this Article, Member States shall encourage the use of co-regulation as provided for in Article 4a(1).

5. 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.

6. Member States may impose on video-sharing platform providers measures that are more detailed or stricter than the measures referred to in paragraph 3 of this Article. When adopting such measures, Member States shall comply with the requirements set out by applicable Union law, such as those set out in Articles 12 to 15 of Directive 2000/31/EC or Article 25 of Directive 2011/93/EU.

7. Member States shall ensure that out-of-court redress mechanisms are available for the settlement of disputes between users and video-sharing platform providers relating to the application of paragraphs 1 and 3. Such mechanisms shall enable disputes to be settled impartially and shall not deprive the user of the legal protection afforded by national law.

8. Member States shall ensure that users can assert their rights before a court in relation to video-sharing platform providers pursuant to paragraphs 1 and 3.

9. The Commission shall encourage video-sharing platform providers to exchange best practices on co-regulatory codes of conduct referred to in paragraph 4.

10. Member States and the Commission may foster self-regulation through Union codes of conduct referred to in Article 4a(2).