Coimisiún na Meán

Coimisiún na Meán Decision Framework on

Hosting Service Provider Exposure to Terrorist Content

1. Introduction

Coimisiún na Meán (the "**Commission**") has been designated as a competent authority under Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online ("**TCOR**" or the "**Regulation**"), for the purposes of Article 12(1)(c).[1] This means the Commission is competent to oversee specific measures taken by a hosting service provider ("**HSP**") within the jurisdiction of Ireland that is deemed to be exposed to terrorist content.[2]

This requires the Commission to determine, on the basis of objective factors, such as the HSP having received two or more final removal orders in the previous 12 months, whether a HSP is exposed to terrorist content (a "**Decision**"). Where its Decision is that the HSP is exposed to terrorist content, the Commission must then notify the HSP.

Terrorist content is content that incites, solicits, threatens or instructs on the commission of terrorist offences. A full definition is set out in the **Annex**.

2. Purpose of this Framework

The Regulation is not prescriptive as to how competent authorities are to arrive at a Decision. The Commission is required to carry out its functions under TCOR in an objective and non-discriminatory manner while fully respecting fundamental rights.[3]

The Commission has prepared this framework ("**Framework**") to detail the process to be followed in order to take a Decision and to set out the key obligations of a HSP following a Decision that it is exposed to terrorist content. A decision framework on these matters supports evidence-based, transparent, consistent and proportionate decision-making by the Commission in the exercise of its statutory functions.

This Framework may be updated or augmented from time to time, to reflect additional processes or considerations associated with the Commission's TCOR responsibilities. It is not a substitute for any statutory provisions and does not constitute legal advice.

---

[1] See SI 545 of 2023: https://www.irishstatutebook.ie/eli/2023/si/545/made/en/print?q=terrorist+content.

[2] Note the Commissioner of An Garda Síochána has been designated as a competent authority under Art 12(1)(a) for the issuing of removal orders pursuant to Article 3 TCOR; see SI 270 of 2023: https://www.irishstatutebook.ie/eli/2023/si/270/made/en/print?q=terrorist+content.

[3] Article 13(2) as transposed by Regulation 4, SI 545/2023.

3. Stages of Decision Framework

The Commission's decision-making process will follow two stages:

Stage 1: Preliminary Decision and Engagement with the Provider

When the Commission becomes aware that a provider, which is a HSP in its jurisdiction, has received two or more final removal orders in the previous 12 months, the Commission will consider the matter and make a preliminary decision (the "**Preliminary Decision**") on whether the HSP is exposed to terrorist content.

Before taking a Decision that a provider is a HSP exposed to terrorist content within the meaning of Article 5(4) the Commission will issue a letter to the HSP setting out the reasons informing the Preliminary Decision and inviting the HSP to provide its comments. The provider may provide its comments to the Commission within a period of three (3) weeks. A provider's failure to respond or engage with the Commission within this stage would not preclude the Commission from taking a Decision based on the existing evidence available to it.

Stage 2: Decision

This stage of the Commission's decision-making process involves taking a Decision, having regard to the information available to it, including any further information received following engagement with a prospective HSP under Stage 1, to take a decision finding that the HSP is or is not exposed to terrorist content.

The Decision will take effect on the Commission issuing the HSP with written notice of the Decision.

4. Consequences of Decision

Following a Decision that it is exposed to terrorist content, a HSP's key obligations are to:

- where applicable, include in its terms and conditions and apply provisions to address the misuse of its services for the dissemination to the public of terrorist content;[4]
- take specific measures to protect its services against the dissemination to the public of terrorist content;[5] and
- report to the Commission, within three months of receipt of the Decision and on an annual basis thereafter, on the specific measures that it has taken and that it intends to take in

[4] See Article 5(1). It must do so in a diligent, proportionate and non-discriminatory manner, with due regard, in all circumstances, to the fundamental rights of the users and taking into account, in particular, the fundamental importance of the freedom of expression and information in an open and democratic society, with a view to avoiding the removal of material which is not terrorist content. Note that Article 2(8) defines "terms and conditions" as "all terms, conditions and clauses, irrespective of their name or form, which govern the contractual relationship between a hosting service provider and its users".

[5] Article 5(2).

order to comply with the obligations set out above.[6]

Specific measures

It is for the HSP to decide which specific measures it will take, although the Commission has a review function (more detail below).[7] The Regulation indicates the measures may include one or more of the following:

(a) appropriate technical and operational measures or capacities, such as appropriate staffing or technical means to identify and expeditiously remove or disable access to terrorist content;

(b) easily accessible and user-friendly mechanisms for users to report or flag to the HSP alleged terrorist content;

(c) any other mechanisms to increase the awareness of terrorist content on its services, such as mechanisms for user moderation; and

(d) any other measure that the HSP considers to be appropriate to address the availability of terrorist content on its services.

The Regulation also requires that the specific measures satisfy the following:[8]

(a) they shall be effective in mitigating the level of exposure of the services of the HSP to terrorist content;

(b) they shall be targeted and proportionate, taking into account, in particular, the seriousness of the level of exposure of the services of the HSP to terrorist content as well as the technical and operational capabilities, financial strength, the number of users of the services of HSP and the amount of content they provide;

(c) they shall be applied in a manner that takes full account of the rights and legitimate interest of the users, in particular users' fundamental rights concerning freedom of expression and information, respect for private life and protection of personal data; and

(d) they shall be applied in a diligent and non-discriminatory manner.

Where specific measures involve the use of technical measures, appropriate and effective safeguards, in particular through human oversight and verification, shall be provided to ensure accuracy and to avoid the removal of material that is not terrorist content.

The Regulation is clear that the requirement to take specific measures:[9]

- is without prejudice to Article 15(1) of the E-Commerce Directive (Now provided for in Article 8 of Directive 2022/2065 (the Digital Services Act)) and shall not entail a general obligation either to monitor information transmitted by a HSP or to actively seek facts and circumstances indicating illegal activity; and

[6] Article 5(5).
[7] Article 5(6).
[8] Article 5(3).
[9] Article 5(8).

- shall not include an obligation for a HSP to use automated tools.

Commission review of specific measures

As above, a HSP must report to the Commission on the specific measures that it has taken and intends to take.

If, based on the reports provided by the HSP or, where relevant, any other objective factors, the Commission considers that the specific measures taken do not meet the HSP's obligations under Articles 5(2) and (3), the Commission shall address a decision to the HSP requiring the necessary measures be taken to ensure that those obligations are complied with. (This does not affect the ultimate ability of the HSP to choose its specific measures.)

5. Duration of Decision - Right to Request Review, Amendment or Revocation

Following a Decision that a HSP is exposed to terrorist content, the HSP may, at any time, request the Commission to review and, where appropriate, amend or revoke a Decision.[10]

In reviewing the Decision, the Commission will take into account any additional information provided by the HSP as part of the request for review. The Commission may also invite the HSP to provide any further information which it may require as part of the review.

The Commission is obliged to notify the HSP of its decision (including reasons) within three months of the request. Its decision must be based on objective factors.

If the Commission decides to revoke a Decision, the HSP's reporting obligations cease. However, if the Decision is upheld, the HSP will be obliged to continue reporting until such time as the Commission deems (upon further request by the HSP) that the HSP is no longer exposed to terrorist content.

[10] Article (5)7.

Annex

Definition of "terrorist content" from Article 2(7) TCOR

Terrorist content means one or more of the following types of material, namely material that:

(a) incites the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, where such material, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed;

(b) solicits a person or a group of persons to commit or contribute to the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;

(c) solicits a person or a group of persons to participate in the activities of a terrorist group, within the meaning of point (b) of Article 4 of Directive (EU) 2017/541;

(d) provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorist offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;

(e) constitutes a threat to commit one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541.

Offences referred to in Article 3(1) of Directive (EU) 2017/541

(1) Member States shall take the necessary measures to ensure that the following intentional acts, as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, are defined as terrorist offences where committed with one of the aims listed in paragraph 2:

(a) attacks upon a person's life which may cause death;

(b) attacks upon the physical integrity of a person;

(c) kidnapping or hostage-taking;

(d) causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;

(e) seizure of aircraft, ships or other means of public or goods transport;

(f) manufacture, possession, acquisition, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of, chemical, biological, radiological or nuclear

weapons;

(g) release of dangerous substances, or causing fires, floods or explosions, the effect of which is to endanger human life;

(h) interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life;

(i) illegal system interference, as referred to in Article 4 of Directive 2013/40/EU of the European Parliament and of the Council (19) in cases where Article 9(3) or point (b) or (c) of Article 9(4) of that Directive applies, and illegal data interference, as referred to in Article 5 of that Directive in cases where point (c) of Article 9(4) of that Directive applies;

(j) threatening to commit any of the acts listed in points (a) to (i).

(2) The aims referred to in paragraph 1 are:

(a) seriously intimidating a population;

(b) unduly compelling a government or an international organisation to perform or abstain from performing any act;

(c) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.

DRAFT DECISION NOTICE

Notice of Decision that [Provider] is exposed to terrorist content

Coimisiún na Meán (the "**Commission**"), in exercise of the powers and duties conferred on it by Article 12(c) of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online (TCOR) and Statutory Instrument No. 545 of 2023, hereby gives notice that it has taken a decision that [Provider] is exposed to terrorist content.

Effective Date

Pursuant to Article 5(4)(b) of TCOR, this decision takes effect upon the Commission giving [Provider] notice of the decision. The effective date of this decision is therefore [date].

Jeremy Godfrey
Chairperson
Coimisiún na Meán

[Date]