Coimisiún na Meán

Article 22 Trusted Flaggers

Guidance Document

Publication date:
16 February 2024

Table of Contents

Introduction

Article 22 of the Digital Services Act ("**DSA**") sets out that providers of online platforms shall take the necessary technical and organisational measures to ensure that notices submitted by Trusted Flaggers ("**TFs**"), acting within their designated area of expertise, through the notice and action mechanisms referred to in Article 16 of the DSA, are given priority and processed and decided upon without undue delay.

The status of 'trusted flagger' shall be awarded, on application by any entity, by the Digital Services Coordinator ("**DSC**") of the Member State where the applicant is established, to an applicant that has demonstrated that it meets all of the following conditions set out in Article 22(2) of the DSA:

(a) It has particular **expertise and competence** for the purposes of detecting, identifying and notifying illegal content;
(b) It is **independent** from any provider of online platforms;
(c) It carries out its activities for the purposes of submitting notices **diligently, accurately and objectively.**

Guide to Award

Coimisiún na Meán has developed this Guide which includes an application form/questionnaire to inform interested entities of its assessment and decision-making process to determine whether an entity meets the conditions set out in Article 22. The Guide supports evidence-based, transparent, consistent, and proportionate decision-making by Coimisiún na Meán in the exercise of its statutory functions.

The aim of the Guide is to help applicant entities (hereinafter referred to as "**you"/ "your"**) to understand what is required of your entity for both the application process and your ongoing obligations with which you must continue to comply following the award of trusted flagger status under Article 22.

The Guide is informed by Irish and European legislation, consultation, data-gathering, and independent research. The Guide is not a substitute for any statutory provision(s) and does not constitute legal advice. You are advised to obtain your own independent legal advice on the relevant statutory provisions.

The Guide divides the conditions into four main sections as follows: (1) General Information; (2) Expertise; (3) Independence; (4) Diligence, Accuracy and Objectivity. These matters are relevant to Coimisiún na Meán's assessment of the conditions set out in Article 22. The application form/questionnaire at page 6 contains a list of **questions** under each section that you must respond to.

> **Section (1)** identifies the **general information** about the entity applying for the award of Trusted Flagger status required by the DSC in order to process and consider your application.
>
> **Section (2)** focuses on questions relating to the **expertise** of your entity and how you will ensure that this expertise is maintained and enhanced over the period of award.
>
> **Section (3)** requests information in relation to the arrangements you will put in place to safeguard your entity's **independence in decision making** (including **financial independence**).
>
> **Section (4)** requests information on your entity's **policies and procedures which demonstrate diligence, accuracy and objectivity** in how you have operated or will operate as a TF.

For each section, we also provide **guidance** to help you understand why we are asking these questions. In the Appendix to this Guide, we provide information regarding **eligibility requirements** to apply for TF status

and a list of the **documentary evidence,** records and documents, that you are requested to submit to support and verify the information and representations you have provided in your application.

You are responsible for demonstrating that your entity satisfies the conditions and you must submit all of the information and the documentary evidence specified in this Guide and/or as may be requested at a later stage by Coimisiún na Meán. It is important that you ensure **full and accurate information** is provided to all of the questions to avoid any delays to the application process.

Coimisiún na Meán will have regard to the information submitted and also information available to it from its own independent information-gathering and research that may be relevant to its **verification** of the information submitted by you at this application stage and to its **continuous assessment** of the Certification Conditions.

It should be noted that, in circumstances where it is established following an investigation that an entity no longer meets the Award Conditions, Coimisiún na Meán is required to revoke the award.

Coimisiún na Meán will review this Guidance every 2 years or more regularly as required.

Completed applications or any queries or requests for clarification in relation to the contents of this Guide should be directed to trustedflaggerapplications@cnam.ie.

Please note that this mailbox supports a maximum file size of **50MB**. If your file exceeds this limit or if you are having difficulties sending a file, please contact the Regulatory Operations team at the email address specified above.

Application Instructions

The application submitted by you must comply with the requirements set out below:

- ***Completed application:*** Please ensure you provide **full and accurate** information to all of the questions asked and include any **documentary evidence** referenced in the appended Schedule.

- ***Additional Information:*** Coimisiún na Meán may also require additional information and/or other documentary evidence following its review of your application in order to assess whether you meet the requirements to be awarded Trusted Flagger status. In addition to the documentary evidence specified you can submit any other information that provides context to the information being supplied or supports the answers provided.

- ***Declaration:*** Your application should include a Declaration signed by a suitable authorised person certifying that the information contained in the application form and documentary evidence is true and correct to the best of that person's knowledge and belief.

- ***Changes:*** You must notify, without undue delay, **any changes to your initial application** and/or to any supplemental information that was provided subsequent to the submission of the initial application as requested by Coimisiún na Meán to support its assessment of whether you met the requirements to be awarded Trusted Flagger status.

- ***Decision:*** Coimisiún na Meán shall endeavour, within three to four months of receipt of all information that enables the application to be processed, to communicate in writing its approval of, or its refusal to approve, the award of Trusted Flagger status. The timeframe indicated is based on Coimisiún na Meán having a complete application and all of the requisite information and supporting evidence to make its determination on certification. Coimisiún na Meán will provide you with a statement of reasons as to why your application for Trusted Flagger status was approved or refused.

- ***Publication:*** The decision and award granted by Coimisiún na Meán will be published on its website. Coimisiún na Meán is required to notify to the European Commission the bodies it has awarded Trusted Flagger status in accordance with Article 22. The European Commission will also publish a list of Trusted Flaggers on its website.

- ***Confidential and Commercially Sensitive Information:*** Any information you consider to be commercially sensitive must be included in a Confidential Appendix and clearly cross-referenced to the relevant sections of this Guide. The reasons why you consider the information to be confidential should be clearly set out.

- ***Freedom of Information****:* Records held by Coimisiún na Meán may be requested by persons under the Freedom of Information Act 2014 ("FOI Act"). The provisions of the FOI Act exempt certain records containing commercially sensitive and other confidential information from publication. Coimisiún na Meán will consult with you in respect of any request received prior to making a decision under the FOI Act.

- ***Personal Data:*** Coimisiún na Meán is obligated and committed to protecting all personal data submitted in accordance with its obligations under the General Data Protection Regulation, the Data Protection Act 2018 and any other applicable data and privacy laws and regulations. Coimisiún na Meán's published policy is at: Coimisiún na Meán | Data Protection (cnam.ie) In this notice, Coimisiún na Meán has requested the name and contact details including email addresses of specified persons. The information collected will be used only for the purposes stated herein.

Appendix 1 - Documentary Evidence

1. General Information

Provide your entity's **founding legal documents** or, if you are a public entity, a link to and an outline of the relevant provisions of law that establish your entity and determine its objectives.

Provide the following documentation and information:

- *The entity's certificate of incorporation*
- *The entity's Constitution*
- *Company registration office details*

2. Expertise and Competence - Detecting, Identifying and Notifying Illegal content.

Provide the following documentation and information:

- *Policies / procedures for the appointment of individuals engaged in flagging activity.*
- *Where individuals are identified, a description of the range of experience and expertise (qualifications, accreditations etc.)*
- *Any records or reports published by your or another entity in relation to previous experience in **detecting, identifying and/or notifying illegal content.***

3. Independence

Organisational Independence

Provide the following documentation and information:

- *For all **members, shareholders and directors** please detail any interests or involvement they have in other entities.*
- *Rules of Procedure on terms of office of TFs and rules on conflicts of interest for all directors, members, employees and TFs.*
- *Code of Ethics or Code of Principles or equivalent.*
- *A copy of the Share Register / Commercial Register.*
- *Shareholders' Agreements.*
- *Illustration, in diagrammatic format, of the group structure, in the case of a group of companies.*
- *Copies of policies or other documents to ensure the **Trusted Flaggers** you appoint are independent of online platforms and their recipients and will make decisions impartially.*

Funding and financial independence

Provide the following documentation and information:

- *Financial reports and audited accounts for the preceding financial year.*
- *For newly created organisations, provisional annual budgets and financing plans for 2 years identifying main items of expenditure and expected sources of revenue.*

- *Affidavit[1] of a director or equivalent position verifying the sources of funding and that no conditions are attached to funding arrangements that would impact on the independence of the bodies or the impartiality of its decision making.*
- *Letters of financial commitment from third parties (where applicable).*
- *Copies of written agreements between the entity and funders.*
- *Copies of the entity's policies on funding.*

4. Trusted Flaggers: Diligent, Accurate, Objective

Trusted Flagging Model: Methodologies, Resources and Technology

Provide the following documentation and information:

- *If your entity has already worked with platforms in flagging content,* ***reports or letters of recommendation from platforms*** *in support of your application.*
- *Documented procedures for detecting, identifying and notifying illegal content.*
- *Copies of correction and complaints policies.*
- *Reports or descriptions of previous activities and campaigns in which the organisation has been involved.*
- *Sample Data protection Impact Assessment*

[1] Sworn statement.

Appendix 2 - Who is eligible to be a trusted flagger?

Recital 61 of the DSA:
TF status should only be awarded to **entities**, and not individuals, that have demonstrated, among other things:

- *that they have particular expertise and competence in tackling illegal content*
- *that they work in a diligent, accurate and objective manner*
- *entities can be public in nature, such as, for terrorist content, internet referral units of national law enforcement authorities or of the European Union Agency for Law Enforcement Cooperation ('Europol'), or*
- *they can be non-governmental organisations and private or semi-public bodies such as the organisations part of the INHOPE network of hotlines for reporting child sexual abuse material and organisations committed to notifying illegal racist and xenophobic expressions online.*
- *industry associations representing their members' interests are encouraged to apply for the status of TFs, without prejudice to the right of private entities or individuals to enter into bilateral agreements with the providers of online platforms.*

With no claim to be exhaustive, designated TFs may be:

- **Industry federations and trade associations**, e.g., Intellectual Property Owners organisations;
- **NGOs,** e.g., consumer-rights organisations, child-protection organisations, human-rights organisations, environmental organisations, animal-rightds organisations, etc.;
- **Members of established fact-checkers networks** (e.g., IFCN);
- **Trade unions**;
- **Non-regulatory public entities** like Internet referral units (Europol) or **regulatory bodies** (with the exception of DSCs;
- **Private or semi-public bodies** (e.g., organisations part of the INHOPE network of hotlines).
- **Networks,** the definition of an entity through Article 22 would not preclude networks or alliances of entities, at national and European levels, from applying.

Appendix 3 – List of Areas of Illegal Content

This list of areas of illegal content has been developed by a subgroup of Digital Services Coordinators in contact with the European Commission to assist in the development of harmonised approaches to the implementation of the DSA.

The list is not exhaustive and is indicative only. The list reflects potential areas of illegal content across the Member States which may constitute areas of expertise for applicant bodies.

- **Animal offenses**
  - Animal harm
  - Unlawful sale of animals and/or wildlife smuggling
  - Other
- **Data protection and privacy violations**
  - Biometric data breach
  - Missing processing ground for data
  - Infringements to the right to be forgotten
  - Data falsification
  - Other GDPR data breaches
  - Other
- **Illegal speech**[2]
  - Defamation
  - Discrimination
  - Hate speech
  - Threats of violence (such as death threats)
  - Holocaust Denial
  - Other
- **Intellectual property and other commercial rights infringements**
  - Copyright infringement
  - Design infringement
  - Sports events rights infringements
  - Geographical indications infringements
  - Patent infringement
  - Trade secret infringement
  - Trademark infringement
  - Counterfeit products
  - Other
- **Negative effects on civic discourse or elections**
  - Foreign information manipulation and interference
  - Information manipulation aimed at affecting sincerity/outcome of elections
  - Other
- **Non-consensual behaviour**
  - Non-consensual image sharing
  - Non-consensual items containing deepfake or similar technology using a third party's features
  - Doxing (publicly providing personally identifiable information about an individual)
  - Other
- **Online bullying/intimidation**
  - Stalking

[2] Including all types of public hate speech, regardless of both medium and content (i.e images, videos, texts, public addresses, etc.).

    - Sexual harassment
    - Other
- **Pornography or sexualized content**
    - Image-based sexual abuse (excluding content depicting minors)
    - Rape and other sexual-based violence (depiction of rape and incitement to rape)
    - Other
- **Offense to minors**
    - Failure to implement age-specific restrictions concerning minors
    - Child pornography/Child sexual abuse material
    - Grooming/sexual enticement of minors
    - Unsafe challenges
    - Other
- **Risk for public security**
    - Provocation or incitement to commit an offense dangerous to public safety.
    - Illegal organizations
    - Risk for environmental damage
    - Risk for public health
    - Terrorist content
    - Other
- **Scams and/or fraud**
    - Inauthentic accounts
    - Inauthentic listings
    - Inauthentic user reviews
    - Impersonation or account hijacking
    - Phishing
    - Pyramid schemes
    - Other
- **Incitement to self-harm**
    - Content promoting eating disorders
    - Incitement to self-mutilation
    - Incitement to suicide
    - Other
- **Illegal scope of access to the platform/content**
    - Failure to implement age-specific restrictions other than those concerning minors
    - Illegal geographical requirements
    - Failure to comply with language requirements
    - Other discriminatory access restrictions
    - Other
- **Unsafe and/or illegal products**
    - Insufficient information on traders
    - Illegal offer of regulated goods and services (eg. health)
    - Sale of non-compliant products (eg. dangerous toys)
    - Illegal drugs and weapons trafficking
    - Illegal practices under consumer protection law
    - Malware and ransomware
    - Other
- **Violence**
    - Coordinated harm
    - Gender-based violence
    - Human exploitation
    - Human trafficking
    - Other