Better Internet for Kids

Applying to become a Trusted Flagger under the Digital Services Act

Good Practice Guide

INHOPE

2025

z

Copyright notice

© European Union, 2025

The Commission's reuse policy is implemented by the Commission Decision of 12 December 2011 on the reuse of Commission documents.

Unless otherwise indicated (e.g. in individual copyright notices), content owned by the EU within this publication is licensed under Creative Commons Attribution 4.0 International (CC BY 4.0) licence. This means that reuse is allowed, provided appropriate credit is given and changes are indicated.

You may be required to clear additional rights if a specific content depicts identifiable private individuals or includes third-party works. To use or reproduce content that is not owned by the EU, you may need to seek permission directly from the rightsholders. Software or documents covered by industrial property rights, such as patents, trademarks, registered designs, logos and names, are excluded from the Commission's reuse policy and are not licensed to you.

Contents

1. Introduction

The Digital Services Act (DSA) aims to provide improved digital safeguards for all users and consumers of digital goods and services in the European Union (EU). Among the new rules imposed, one key highlight of the DSA is the increased priority status and institutionalisation of Trusted Flaggers in the EU. The DSA gives more responsibilities and power to recognised Trusted Flaggers by creating a legal obligation for companies to act rapidly on reports of illegal content received by them. Trusted Flaggers can include non-governmental organisations, helplines, hotlines, child welfare organisations, and other entities with expertise in detecting illegal content. This guide offers practical advice for organisations seeking Trusted Flagger status under the DSA.

INHOPE is a leading global network of hotlines dedicated to combatting online child sexual abuse material (CSAM). INHOPE member hotlines have decades of experience in identifying, processing and removing harmful and illegal content from the internet. In addition, many member hotlines have already established partnerships with online service providers, serving as recognised "trusted flaggers" or trusted reporters. The INHOPE network's high-quality standards and extensive experience optimise member hotlines for Trusted Flagger status.

This guide explains the key requirements and offers practical advice for organisations, such as hotlines and helplines, that wish to apply for Trusted Flagger status under the DSA. It includes sample questions and examples of information that applicants can provide to show compliance with the conditions set out in Article 22(2) of the DSA. Although the examples are drawn from hotline practices and policies, they can also serve as useful guidance for helplines and other child welfare organisations interested in applying. The guide also briefly outlines the ongoing obligations that organisations must continue to meet once Trusted Flagger status has been granted. It is important to note that this guide serves as an advisory tool and does not impose any mandatory rules for application. The application format and required information may differ by country, depending on their national Digital Services Coordinator

(DSC). Please consult your national DSC for specific application format or requirements.

1.1. Digital Services Act (DSA)

The Digital Services Act (DSA) entered into enforcement on 17 February 2024, as part of the Digital Service Package proposed by the European Commission (EC).

The DSA aims to create a safer digital space by protecting fundamental rights of users and creating horizontal due diligence obligations for providers of intermediary services. As part of its regulatory toolbox, the DSA facilitates tackling illegal content online. It applies to and regulates online platforms, hosting services, other online intermediaries[1], Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) operating in the EU. These online service providers have to comply with obligations under the DSA for higher transparency and accountability, including, for example, responsibilities to tackle illegal content and provide transparency about content moderation and their online marketing practices.

A key distinction within the DSA is the graduated regulatory framework:

- Online platforms are subject to baseline obligations that include having notice-and-action mechanisms (Article 16), transparency reporting, complaint and redress systems, and special protections for minors.
- Very Large Online Platforms (VLOPs), defined as platforms with more than 45 million active users in the EU, are subject to stricter and more extensive obligations, given their systemic impact on society. These include requirements to conduct annual risk assessments (Article 34) on the dissemination of illegal content, mitigation of systemic risks (Article 35), external independent auditing (Article 37), and ensuring access to real-time data for vetted researchers (Article 40).

[1] Online platforms include online marketplaces, app stores, collaborative economy platforms, social networks…etc. Hosing services include cloud services and webhosting. Other online intermediaries include internet access providers, domain name registries…etc.

As of August 2024, 23 VLOPs and 2 VLOSEs have been designated by the EC[2], and thus facing additional due diligence obligations under the DSA. The compliance with those obligations is monitored by the EC.

One of the obligations under the DSA is to require online platforms to put in place appropriate measures to sufficiently protect minors on their services. Online platforms are obligated to remove CSAM and other non-consensual sexual content in a timely manner (Article 16), adopt a high level of safety, privacy and security settings by default for children (Article 28 (1)), and precludes online platforms from presenting targeted advertisements based on profiling children (Article 28 (2)).

In addition, all Member States in the EU have to appoint their Digital Services Coordinator (DSC) as the main body responsible for the national implementation of the DSA. A list of appointed DSCs in each EU country can be found in Annex I.

For more information about the DSA, please refer to the European Commission website and the DSA Transparency Database, which makes all statements of reason provided by providers of online platforms for their content moderation decision accessible to the public.

1.2. Trusted Flaggers under the DSA

One of the features of the DSA is the priority given to notifications of illegal content submitted by Trusted Flaggers, enabling faster and more effective action against illegal content. While providers of online platforms shall put mechanisms in place for Notice and Action of illegal content in accordance with Article 16 of the DSA, the notices submitted by Trusted Flaggers through such mechanism will be "given priority and are processed and decided upon without undue delay" (Article 22). This creates a legal obligation for companies operating within the EU to cooperate with recognised Trusted Flaggers and rapidly act on reports received by Trusted Flaggers.

[2] Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) are those with over 45 million users per month in the EU. Once designated by the EC, VLOPs and VLOSEs have the obligations to comply with the DSA within four months. They also have to publish their first transparency reports including the additional transparency requirements at the latest six months after their designation. In addition, they must publish their transparency reports at least every six months, including information on content moderation and actions taken. See the full list of designated VLOPs and VLOSEs here.

Article 22 of the DSA is the primary provision outlining details regarding Trusted Flaggers. Trusted Flaggers are entities with particular expertise and competence in detecting, identifying and notifying illegal content.[3] They can be non-governmental organisations, consumer organisations, and semi-public bodies. They should also be independent from any provider of an online platform, and they must carry out their activities in a diligent, accurate and objective manner (Article 22(2)(c)). In particular, Recital 46 explicitly mentioned "organisations part of the INHOPE network" as an example of a type of organisation which can become a Trusted Flagger.

Trusted Flaggers are required to maintain independence from any online platform provider and conduct their activities diligently, accurately, and impartially (Article 22(2)(c)). In terms of obligations, Trusted Flaggers should publish easily comprehensible and detailed reports at least once a year on notices submitted in accordance with Article 16, with an explanation of the procedures in place to ensure that the trusted flagger retains its independence. These reports should be made publicly available and sent to national DSC (Article 22 (3) and Recital 46).

[3] Recital 46, "(s)uch 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, consumer organisations and 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. For intellectual property rights, organisations of industry and of right-holders could be awarded trusted flagger status, where they have demonstrated that they meet the applicable conditions and respect for exceptions and limitations to intellectual property rights."

2. Applying to Become Trusted Flaggers

2.1. Application Process

Any interested entities that meet the requirements under Article 22 of the DSA can apply to become Trusted Flaggers. The status of Trusted Flagger will be assessed and awarded by the Digital Services Coordinator of each member state in the EU.

It is recommended to check with your national Digital Services Coordinator on the detailed information about the application process and application forms. The section below provides sample questions and answers to demonstrate your expertise and competence as required in the DSA.

2.2. Sample Application Questions and Answers

Article 22 (2) of the DSA sets out three conditions for Trusted Flaggers. An interested entity should demonstrate that:

(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**. (Article 22 (2), DSA)*

This part of the Guideline is therefore developed with questions that interested entities may need to answer, and information to provide to demonstrate compliance with the above three conditions. In addition to this, an interested entity should also provide relevant general information about its organisation in the application, including but not limited to entity type, mission and relevant activities and the structure of the entity.

2.2.1. Expertise and Competence: Detecting, Identifying and Notifying Illegal content.

Sample questions and information to provide

1. List the specific area/s of illegal content in which your entity has flagging expertise.

Information to provide:

Organisations seeking Trusted Flagger status must demonstrate their expertise in detecting, identifying, and reporting illegal content. This includes, but is not limited to, content such as CSAM, illegal hate speech, cyberbullying, and other forms of illegal online behaviour. The following organisations may apply:

- Hotlines: Typically focused on illegal content related to CSAM, human trafficking, child exploitation, etc.
- Helplines: Offer support and report on a range of harmful content, including cyberbullying, self-harm, and suicide-related material.
- Child Welfare Organisations: Often involved in detecting illegal content that affects minors, such as grooming, child pornography, or exploitation.

Hotlines, helplines, and child welfare organisations may have expertise in flagging illegal or harmful content such as:

- CSAM
- Child trafficking and exploitation
- Child grooming activities
- Hate speech
- Cyberbullying
- Sexual extortion
- Suicide and self-harm material

- Extremist content
- Terrorism

Within your application, you should detail specific types of illegal content your organisation has flagged, especially focusing on content like CSAM, illegal hate speech, or other categories that align with DSA objectives.

2. What prior experience does your entity have in detecting, identifying and notifying illegal content?

Information to provide:

Hotlines, helplines, and child welfare organisations have extensive experience in reporting illegal content, particularly CSAM, to authorities or hosting service providers to have them removed. This includes the use of secure online platforms for reporting and regularly collaborating with law enforcement agencies.

INHOPE member hotlines have extensive experience ensuring that illegal content, in particular CSAM online, is taken down and criminal offences are reported to the authorities. INHOPE hotlines receive public reports on suspected illegal content from the public through online reporting forms on hotlines' websites. These reports are then analysed everyday by hotline analysts. If the content is classified as illegal and hosted in the country, hotlines will notify law enforcement agencies for further investigation, and a Notice and Takedown (NTD) order will be sent directly to the hosting providers, either by the hotlines themselves or by national law enforcement agencies. INHOPE hotline analysts are trained on content classification by both INTERPOL and INHOPE. If the content is hosted outside the country, hotlines forward the report through ICCAM, a technology platform used by the INHOPE network to exchange reports between hotlines. Thus, as part of the global INHOPE network, hotlines collaborate with other hotlines on a regular basis to exchange reports, expertise and build collaboration.

(Please include here relevant statistics such as number of reports received, the percentage of CSAM reports and other relevant numbers to demonstrate your expertise. You can also link your annual report to show comprehensive data.)

Hotlines and helplines have well-established and trusted relationship with national hosting providers and industry partners. Additionally, many hotlines maintain a strong relationship with national law enforcement through periodic coordination meetings with their law enforcement agencies and relevant national stakeholders. Hotlines also stay in regular contact with the law enforcement agencies outside of these coordination meetings.

a. Has your entity joined Trusted Flagger/ Trusted Partner programme of any online platforms? If yes, describe the experience.

Information to provide:

Many INHOPE hotlines and child welfare organisations have been trusted reporters for platforms like Google, Facebook, and TikTok. They follow each platform's specific reporting mechanisms and maintain close communication to ensure swift action on reported content. Each platform has its own method for trusted reporters to flag illegal content to them, such as sending emails to a contact person, using the designated online reporting form or an API (Application Programming Interface connecting two systems). Hotlines and helplines adhere to each platform's preferred reporting method. Regardless of the method, trusted reporters maintain close contact with these platforms and can reach out to a designated contact person for follow-up in case of non-responsiveness.

Some hotlines do internal monitoring on the NTD notices and follow-up process of reported illegal content. This way, hotlines are able to track whether reported content is taken down in a timely manner. If hotlines don't receive a confirmation of the removal of a reported content, hotlines may send reminders to the hosting provider. If no actions are taken after the reminder, hotlines may then organise a meeting with the hosting provider or notify LEA.

(Suggestion to include: Relevant statistics such as the number of notifications/ reports sent to online service providers by your organisation under such programme/ partnership, the number of notifications/ reports that were actioned by online service providers, the number of notifications/ reports that were denied by online service providers…etc.)

3. What other prior experience does your entity have that may be relevant?

Information to provide:

INHOPE hotlines have experience in conducting research and participating in various projects. Some examples include:

- Study on Sexual Harassment in Communication on Social Media by jugendschutz.net
- Project Indicators by ECPAT Sweden to detect and prevent payments for Livestreamed Child Sexual Abuse
- CSAPE Project led by Save the Children Finland and funded by the EU on preventing child sexual abuse through sexual education.

In addition, hotlines in the EU are part of the EU co-funded network of Safer Internet Centres (SICs) and work in collaboration with helplines and awareness raising centres, on various projects, campaigns and studies aimed at creating a safer online environment for children. SICs also conduct research and create resources that are made available on the Better Internet for Kids (BIK) website. Since entering into force of the DSA, the EU co-funded SICs have been actively providing support to **the Commission in** the enforcement of the DSA based on the evidence they gather in regards children and young people’s experiences and concerns, as well as **online trends and harms occurring in the EU**.

4. What are the methods and technology used for detecting, identifying and notifying illegal content?

Information to provide:

INHOPE hotlines receive reports of alleged illegal content through public reporting. Once a public report is received, hotline analysts insert the URL of the report into ICCAM, which is a secure technology platform used by the INHOPE network. The system then crawls all information found on that URL, and the analyst classifies each picture and/or video separately as baseline (internationally illegal according to INTERPOL's criteria), nationally illegal (according to national legislation in the hosting country) or not illegal. If the content is classified as illegal and hosted in the country, hotlines inform the national law enforcement agency and send a Notice and Takedown order to the relevant hosting provider. If the content is classified as illegal but hosted outside the country, hotlines send the report to the hotline in the relevant country through ICCAM.

In addition, reports inserted into ICCAM by INHOPE hotlines contribute to INTERPOL's International Child Sexual Exploitation Image Database (ICSE Database).

5. What personnel trainings does your entity provide for analysts/ individual engaged in flagging activities?

Information to provide:

All hotline staff members in the INHOPE network participate in INTERPOL-INHOPE content assessment trainings, advanced analyst trainings and hotline training meetings every year. They also join the INHOPE monthly Q&A online sessions to exchange expertise and issues with other INHOPE analysts. In addition, they attend a series of online webinars every year to be informed about latest technological trends, CSAM trends, crime tactics and new tools. All hotlines have access to INHOPE's best practice papers, templates and manuals ensuring high quality of practices within each member hotline. These resources are based on best practices within the network globally.

Suggested attachment

1. Any statistics or reports published relating to previous experience in detecting, identifying and/or notifying illegal content.

2. Previous annual reports demonstrating the entity's expertise and experience in the field of certain illegal content.

2.2.2. Organisational Independence

Sample questions and information to provide

1. **Describe the structure of your entity:**
   - 1a. **Is your entity a company in a larger company group structure? If yes, provide details of this group.**
   - 1b. **What is your entity's relationship with, or interests in, any other undertakings?**
   - 1c. **Who are the directors of the Board of your entity and do any of the directors sit on the Board in a representative capacity for any of your shareholders?**

Information to provide:

The structures of hotlines, helplines, and child welfare organisations vary based on the nature of the organisation, whether they are civil society organisations, industry-led initiatives, or governmental agencies. These organisations may also include NGOs, charities, or public service entities.

Regardless of the structure, all these organisations, whether hotlines, helplines, or child welfare bodies, have relationships with major stakeholders in their country of operation, which may include government bodies, law enforcement, internet industry representatives, child protection groups, and other relevant entities. These relationships are often governed by specific codes of practice or service agreements that ensure compliance with national and international regulations, as well as collaboration on issues like online safety, content moderation, and children's rights protection.

Please provide a detailed description of your organisation's structure, including your governing body, any affiliations, and the key stakeholders you work within the context of your operations.

2. Are there any policies/ procedures to ensure organisational independence?

Information to provide:

Prospective applicants should have the following documents in place to ensure good and effective operation:

1) Article of Association: The Article of the Association outlines the governance structure of the organisation, operational procedures and membership detail.
2) Code of Ethics: The Code of Ethics outlines the values, standards and rules of behaviours expected within the organisation. A key element of the Code of Ethics is to remain professional and independent in the workplace, prohibiting any behaviour that compromises integrity or involves conflicts of interest. It also outlines principles for managing conflicts of interest that may arise.
3) Rules of Procedure: The Rules of Procedure outline the report-handling process of public reports. All reports received are dealt with by hotline analysts according to these Rules of Procedure.
4) Member or Partnership agreements: Written agreements laying down partnership detail including rights and responsibilities signed by both parties.
5) Complaint Procedure: INHOPE hotlines are required to have a clear procedure on how any interested person can make a complaint about the work of the hotline or hotline analysts, as well as an internal complaints and whistleblowing procedures that are made aware to all employees. The two complaint procedures ensure that complaints from users or any stakeholders are addressed promptly, fairly, and transparently.

3. Provide detail on organisational independence—personnel independence:

a. How will you ensure that flaggers are independent of online platforms and will remain so for their term of office?

b. How will you ensure that flaggers undertake their activities in an impartial and objective manner?

Information to provide:

Hotline analysts undergo a comprehensive background check as part of the recruitment procedure. All analysts adhere strictly to their hotline's Code of Ethics and Hotline Rules of Procedures in their daily tasks, including flagging content and notifying hosting providers and online platforms. In addition, hotline analysts receive regular trainings and evaluations to maintain impartiality and objectivity in their work.

All INHOPE hotlines are bound by their mission above all and operate independently of any single platform's influence. They strictly adhere to INHOPE Code of Practice and membership requirements and undergo a periodic quality assurance review under INHOPE's Quality Assurance Programme. During this review each hotline is assessed on compliance with INHOPE's Articles of Association, Code of Conduct and Best Practice Papers. Upon successful review, hotlines receive a certificate. Each hotline is reviewed every three years at a minimum.

4. Provide detail on organisational independence—independence from service providers:

a. What are the current relationships or channels with online platforms?

Information to provide:

All hotlines, helplines, and child welfare organisations have relationships with hosting providers, which is typically required by their respective codes of practice or operational guidelines. The nature and depth of these relationships can vary depending on the specific organisation type and their function in detecting, reporting, and handling illegal content.

1. For organisations that are operated by membership associations, such as hosting provider associations or other child welfare groups, it is possible that online platforms may be members of the association. However, these membership relationships do not create a conflict of interest, as organisations strictly adhere to their established Rules of Procedure when analysing and

flagging illegal content. This ensures that all content is processed objectively, without any undue influence from member organisations.

2. For organisations that are already trusted flaggers or trusted reporters for online service providers, they maintain close contact with hosting providers and other online platforms under such agreements. This allows these organisations, whether hotlines, helplines, or welfare bodies, to quickly resolve issues by reaching out to the relevant hosting provider or platform. The communication channels between organisations and online platforms vary, including designated email addresses, online forms, online portals, and automated tools. These communication methods are formalised and traceable to ensure accountability and transparency in content reporting.
3. Online service providers are often partners with these organisations when running awareness-raising campaigns or conducting relevant research studies. These partnerships are built on mutual support, information sharing, and maintaining integrity. While these collaborations are important for raising awareness and fostering safer online environments, they do not influence the operational independence of the organisation in flagging and reporting illegal content.

Suggested attachments

1. Code of Ethics/ Principles
2. Rules of Procedure regarding managing conflicts of interest for members of your entity and staff or individuals engaged in flagging activity.
3. Financial reports and audited accounts for the preceding financial year
4. Annual Reports outlining the activities and governance of the organisation.
5. Pre-existing contract/agreement with any online platform(s) or other external sources of funding
6. List and information of the Board of Directors, including public information about the governance of the organisation.
7. Recruitment procedures

2.2.3. Work done for the purposes of submitting notices diligently, accurately and objectively.

Sample questions and information to provide

1. **Provide full details of the methodology to detect, identify (and assess) and notify illegal content.**
   1a. **Procedures (including standards of assessment), tools and systems you use or will use.**
   1b. **Details of human resources**

Information to provide:

The standard procedure INHOPE hotlines take when receiving a report of alleged child sexual abuse material is as follows:

1) Public report is received through the hotline's online reporting form on the website, built with a report management system (e.g. INHOPE's friendly plug-in website tool Report Box).

2) Analysts insert the URL of the report to ICCAM. ICCAM crawls the webpage inserted and shows all the pictures and videos displayed on the page. ICCAM also shows the hosting country of the report URL and the URLs of the images and videos. Analysts classify the pictures and videos as baseline (illegal globally), nationally illegal, undetermined (requires further review) or not illegal.

3) If the report is classified as illegal and hosted within the country, the hotline informs national law enforcement agencies. A Notice and Takedown order will be sent to the relevant hosting provider. If the report is not hosted in the country, the hotline sends the report to the relevant hotline in the hosting country through ICCAM. The hotline in the hosting country ensures that the national law enforcement agency is notified, and a Notice and Takedown order is sent to the relevant hosting provider located within their country.

INHOPE hotline analysts follow the ICCAM User Manual and Process Operations Manual and participate in INTERPOL content assessment trainings to ensure that reports are processed accurately and diligently. In addition to using ICCAM, INHOPE hotlines also use various technological tools to assist them in receiving, processing and analysing CSAM reports, such as Report Box, APIs and SCARt.

2. How will you ensure accuracy?

2a. Detail the number and quality of the sources of evidence that will be used in the flagging activity and the sources' possible vested interest

2b. Detail the correction policy you will use

Information to provide:

Accuracy can be ensured through an appeal process established by hotlines. If a hosting provider challenges the validity of an NTD notice, the hosting provider can contact the hotline and the report will be reviewed by another analyst, such as the senior analyst or the hotline manager. In the case of CSAM, the hotline can consult the law enforcement agency. If a new decision is made, the hosting provider and the law enforcement agency will be informed about it.

3. Detail the criteria you will apply for triaging illegal content detected and notified to the platform.

Information to provide:

Regarding CSAM reports, INHOPE hotlines generally classify the material using three criteria: "baseline" which is internally illegal according to INTERPOL's criteria, "nationally illegal" which is illegal according to the national law in the country, and "not illegal". If the content is baseline and nationally illegal, the hotline will inform law enforcement and send a NTD to the relevant hosting provider. All images and videos marked as baseline and nationally illegal are also made available to INTERPOL through ICCAM. INTERPOL downloads this material and transfers it for insertion into their International Child Sexual Exploitation Image Database (ICSE Database).

Regarding the determination for sending reports as Trusted Flaggers to online service providers, this would involve assessing based on national illegality or breaches of the terms of service agreed upon with the industry partner. If these criteria are met, the report is then forwarded to relevant online service for content removal.

4. Explain your policies or equivalent in relation to the health, safety and wellbeing for flaggers in your entity.

Information to provide:

All INHOPE hotlines are required to establish a staff welfare policy, as one of the requirements to receive the INHOPE quality assurance certification. INHOPE's Staff Welfare best practice paper outlines policies that should be followed to ensure the wellbeing of all staff, including:

1) The maximum working hours for report handling per person and screen break
2) Secure work environment, including physical, electronic and personal security
3) Mandatory professional psychological support or counselling
4) Other welfare support including team building, the flexibility to work from home and harm minimisation

5. Provide details of any reviews conducted in respect of flagging activity

Information to provide:

Reviews can be conducted through monitoring of the NTD notices sent with an internal tracking system. If no confirmation of the takedown of the content is received, hotlines can send another reminder and continue to follow-up on it.

Reviewing only takes place when the hosting provider challenges the validity of the NTD notice. The hosting provider can contact the hotline and the report will be reviewed by the senior analyst and hotline manager. In the case of CSAM, the hotline can also consult the law enforcement agency. In practice, no appeals or challenges have been raised by hosting providers regarding CSAM reports in the past 10 years.

Suggested attachment

6. Reports or letters of recommendation from platforms in support of your application
7. Correction and complaints policies
8. Staff welfare policies
9. Reports or descriptions of previous activities and campaigns in which the organisation has been involved.

3. Maintaining Trusted Flagger Status

3.1. Duties of Trusted Flagger

Trusted flaggers are responsible for detecting potentially illegal content and sending notices to online platforms under the DSA.

Article 22 (3) of the DSA further lays out the reporting duty of trusted flaggers:

Trusted flaggers shall publish, at least once a year easily comprehensible and detailed reports on notices submitted in accordance with Article 16 during the relevant period. The report shall list at least the number of notices categorised by:

(a) the identity of the provider of hosting services,

(b) the type of allegedly illegal content notified,

(c) the action taken by the provider.

Those reports shall include an explanation of the procedures in place to ensure that the trusted flagger retains its independence.

Trusted flaggers shall send those reports to the awarding Digital Services Coordinator and shall make them publicly available. The information in those reports shall not contain personal data.

3.2. Maintaining Diligence and Objective Submission

Awarded trusted flaggers should maintain due diligence, and accurate and objective submission of notices. If this criterion is not met, it is possible to lose the trusted flagger status. Article 22 (6) of the DSA states the following:

Article 22 (6): "Where a provider of online platforms has information indicating that a trusted flagger has submitted a significant number of insufficiently precise, inaccurate or inadequately substantiated notices through the mechanisms referred to in Article 16, including information gathered in connection to the processing of complaints through the internal complaint-handling systems referred to in Article 20(4), it shall communicate that information to the Digital Services Coordinator that *awarded the status of trusted flagger to the entity concerned, providing the necessary explanations and supporting documents. Upon receiving the information from the provider of online platforms, and if the Digital Services Coordinator considers that there are legitimate reasons to open an investigation, the status of trusted flagger shall be suspended during the period of the investigation. That investigation shall be carried out without undue delay."*

Suggested practices for maintaining trusted flagger status

After becoming a trusted flagger, it is crucial to sustain the level of performance, accuracy, and transparency expected under the DSA. The following practices can help maintain trusted flagger status.

Annual Reporting and Transparency

- **Develop a Standardised Reporting Format:**
  - Create a structured template for your annual report, categorising the data as required by the DSA: listing content types flagged, actions taken by service providers, and follow-up processes.
  - Reporting Considerations: Document each notice's impact, including the response rate from platforms and any notable delays in action. Detail steps taken to address any rejections or appeals to strengthen transparency.
- **Publish Reports for Public Access:**
  - In addition to submitting the report to your DSC, ensure public accessibility (e.g., on your website) to build trust. Make sure that sensitive information is anonymised or summarised to comply with data protection requirements.

Regular Staff Training and Quality Assurance

- **Prioritise Consistent Training:**
  - Develop a regular training schedule for analysts and staff engaged in content detection. Focus on DSA-relevant issues like flagging

objectivity, content classification, and platform-specific flagging procedures.

  - Consider mandatory refresher sessions covering recent illegal content trends, technological advancements in content moderation, and updates to the DSA.

- **Implement Quality Assurance (QA) Audits:**
  - Conduct QA reviews quarterly or biannually to identify potential gaps in flagging accuracy or process efficiency.
  - Attachment Recommendations: Attach any QA audit reports or summaries of improvements implemented based on audit findings.

Data and Documentation of Impact

- **Track Key Metrics:**
  - Collect data on the effectiveness of your flagging activities, such as the number of flagged content pieces, response time, and content removal rates. Regular tracking highlights your impact and assists with renewal applications.
  - Suggested Data Points: Break down metrics by type of illegal content, platform responses, and law enforcement actions taken. Use visualisations like charts in annual reports to make data accessible and impactful.
- **Establish Feedback Loops:**
  - Develop a system for feedback from platforms, DSCs, and internal team reviews to continuously improve accuracy. This feedback could come from platform responsiveness metrics, law enforcement agency updates, or internal flagging reviews.

Preparation for Investigations by Digital Services Coordinators

- **Implement Protocols for Investigations:**

  - Establish clear response protocols for any DSC-initiated investigations into your flagging accuracy or impartiality. Document steps for internal review, appeals, and corrective actions to maintain transparency.
  - Internal Documentation: Track the reasons for flagged content that has been reviewed or challenged by platforms to assess potential areas for improvement and prevent future issues.
- **Conduct Internal Audits Regularly:**
  - Perform internal accuracy audits to pre-empt DSC reviews. This includes verifying the content classification and following up on cases where flagged content was not removed.

4. Annex

4.1. Annex I—List of Digital Services Coordinators in EU Countries

Please see the official Digital Services Coordinator list published by the EC here.

Please refer to the document with information on INHOPE hotlines appointed as Trusted Flaggers here.

Please note that the list below has been last updated at the point of publication of this document.

Country	Digital Services Coordinator
Austria	Communications Authority (KommAustria)
Belgium	Flemish Media Regulator
Bulgaria	Communications Regulation Commission
Croatia	Croatian Regulatory Authority for Network Industries (HAKOM)
Cyprus	Cyprus Radiotelevision Authority
Czech Republic	Czech Telecommunication Office (ČTÚ)
Denmark	Danish Competition and Consumer Authority
Estonia	Consumer Protection and Technical Regulatory Authority (CPTRA)
Finland	Finnish Transport and Communications Agency (TRAFICOM)
France	Regulatory Authority for Audiovisual and Digital Communication (ARCOM)
Germany	Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways (BNetzA)

Greece	Hellenic Telecommunications & Post Commission (EETT)
Hungary	National Media and Infocommunications Authority (NMHH)
Ireland	Media Commission
Italy	Authority for Communications Guarantees (AGCOM)
Latvia	Consumer Rights Protection Centre (PTAC)
Lithuania	Communications Regulatory Authority of the Republic of Lithuania (RRT)
Luxembourg	Competition Authority
Malta	Malta Communications Authority (MCA)
Netherlands	Authority for Consumer and Markets
Poland	Office of Electronic Communication (TBC)
Portugal	National Communications Authority (ANACOM)
Romania	National Authority for Management and Regulation in Communications (ANCOM)
Slovakia	Council for Media Services (Rada pre mediálne služby)
Slovenia	Agency for Communication Networks and Services of the Republic of Slovenia (AKOS)
Spain	National Commission for the Markets and Competition (CNMC)
Sweden	Swedish Post and Telecom Agency (PTS)

4.2. Annex II—INHOPE Best Practice Papers

Below are INHOPE's Best Practice Paper that can support the Trusted Flagger application. Please note that these best practices papers are only accessible for INHOPE hotlines via the INHOPE member portal or for helplines by request to info@inhope.org.

1. INHOPE Code of Practice
2. INHOPE Best Practice Paper—Notice and Takedown
    a. Explanation—What is Notice and Takedown order
3. INHOPE Best Practice Paper—Staff Welfare
4. INHOPE Best Practice Paper—Recruitment Principles
5. INHOPE Best Practice Paper—Relationship with LEA
    a. MoU
6. INHOPE Guidelines on Complaint Procedure Mechanism
7. INHOPE Security Requirements
8. INHOPE Best Practice Paper— Exchange of reports
9. Minimum Standard Hotline Web Reporting Form
10. ICCAM Process Operation Manual
11. Maturation and Content Assessment Manual

For INHOPE members, please log in to your account to the Member Portal to access the documents.

4.3. Annex III—External Resources

Below are some external resources that can support the Trusted Flagger application.

Digital Services Act Overview and Guidance

- **European Commission - Digital Services Act (DSA) Official Information**
  Overview of the DSA, including the full legal text, updates, and guidance documents from the European Commission. This is the primary source for understanding DSA's obligations.
  - Digital Services Act - European Commission
- **DSA Transparency Database**
  This database provides insights into content moderation practices under the DSA, showing how online platforms handle flagged content.
  - DSA Transparency Database - European Commission

Organisational Independence and Compliance

- **OECD – Creating a Culture of Independence**
  Although not specific to digital services, these guidelines provide general principles on maintaining independence in organisational practices for regulators, which can be adapted for DSA compliance.
  - OECD Guidelines on Independence
- **European Data Protection Board (EDPB) - Data Protection and Privacy Guidelines**
  For Trusted Flaggers, maintaining data privacy is critical. The EDPB offers comprehensive guidelines and best practices for handling personal data securely.
  - European Data Protection Board (EDPB) - Data Protection Guidelines

better-internet-for-kids.europa.eu

@Insafenetwork
@safeinternetday

facebook.com/saferinternet
facebook.com/SaferInternetDay

linkedin.com/company/better-internet-for-kids

youtube.com/@betterinternetforkids

info@betterinternetforkids.eu

Better Internet for Kids