TRUSTED FLAGGER APPLICATION LIST OF SUPPORTING DOCUMENTS

This document describes the type of documentation and information that applicants for the status of trusted flaggers, in the sense of Article 22 DSA, may enclose with their application. A distinction is made between more essential documentation and additional supporting documents that can further back the application.

If the information is publicly accessible, a reference to the web link may suffice. The information may also be provided in a bundled form rather than in separate documents.

If you deliver a document containing information you consider confidential, please also provide a non-confidential version of this document at the same time. In the confidential version, the confidential text elements must be clearly indicated.

1. Admissibility of the application

Proof that the candidate possesses legal personality and is not a natural person (private persons are excluded), as well as that the candidate is established in Belgium.

1. Memorandum of association and/or articles of association;
2. Company data (such as the company number in the Crossroads Bank for Enterprises, the location of the headquarters, etc.);
3. Representation mandate or a declaration under oath as proof of a valid mandate to bind the entity, if this is not evident from the articles of association.

2. General information/mission (statement)

1. Mission statement (possibly from the articles of association);
2. Where applicable: general terms and conditions of the entity;
3. If flagging is a new activity for the entity: description of the motivation for or importance of becoming a trusted flagger.

3. Particular expertise and competence for the purposes of detecting, identifying and notifying illegal content

3.1 Of the entity in general

1. Proof of a designated area of expertise and necessary language skills;
2. Where applicable, evidence of (previous) cooperation as a flagger with online platform provider(s) prior to the existence of the DSA, including the agreement with those online platform provider(s);
3. Description of the processes, procedures or strategies used to create notifications (e.g. modus operandi, flow chart, …);

4. Use of tools (IT programs, tools for detecting/monitoring illegal content, detecting trends, tools to ensure the secure processing of information, in particular illegal content and personal data, other mechanisms…);
5. Training material for personnel: evidence of training in identifying illegal content, knowledge of the relevant legal standards (e.g. DSA, national legislation), assessment of reports, …

Additional documentation:

6. Publications: studies, annual reports, opinions, recommendations showing notifications to online platforms, etc.;
7. Anonymised examples of previous notifications, sample reports submitted to online platforms or authorities;
8. Proof of membership/cooperation with expert bodies or networks such as INHOPE, Europol, cybercrime units, independent fact-checking networks, EU Internet Forum, …;
9. Policies or procedures for the recruitment and selection of persons who will carry out flagging activities, and once in service their evaluation and follow-up;
10. Other data that demonstrates previous experience in detecting, identifying and/or reporting illegal content.

3.2 Of the team that will perform the task of trusted flagger

1. Presentation/organisational chart of the structure/organisation of the team (e.g. size of the team, number of full-time equivalents employed, volunteers, etc.);
2. Profiles, CVs of the staff concerned, including specific training and diplomas in the specific area of expertise.

Additional documentation:

3. Certificates obtained or specific training courses taken: e.g. legal/compliance certificate for content moderation, data protection, digital law, cyber security, digital security, programs followed regarding content policy of online platforms, etc.;
4. Contributions made by these people to studies, forums, seminars, workshops, etc. regarding the areas of expertise;
5. Information about custom office space, teleworking possibilities.

4. Independence from any provider of online platforms

4.1 Organisation

1. Organisational chart of the entity's policy bodies, and in the case of a group of undertakings, a schematic illustration of the group structure;
2. Description of the members of the board of directors, shareholders or members of the association (with or without control, including their relations, as laid down in any shareholders' or stakeholder's agreement). The interests or involvement of all stakeholders – members, shareholders and directors – in online platform provider(s) should be indicated, where appropriate;
3. Decision-making rules (internal rules, voting rights, etc.) and description of the decision-making process for flagging activities, as well as documents demonstrating the independence of the entity and the staff from online platforms and impartiality in decision-making;
4. Internal rules or procedural rules in the event of conflicts of interest, or an ethical code;

5. Description of contracts and partnerships with online platform provider(s), including a declaration of independence.

Additional documentation:

6. Independent research or general policy recommendations based on which can be inferred that there is no influence exerted by online platforms.

4.2 Financial

1. Annual accounts, at least for the last two years;
2. In the case of a newly created entity: financial business plan or budget plan;
3. Description of all sources of funding (subsidies, donations, membership fees, etc.);
4. Where applicable: agreements with partners, sponsors and/or investors, including a description of the financial commitments, showing that their (financial) support does not affect the policy or decisions (in the case of confidentiality clauses, to be shared on a confidential basis).

Additional documentation:

5. Where available, an external audit confirming financial independence;
6. Description of how the candidate makes its funding reports public (e.g. a link to the publication on its website).

5. Diligence, accuracy and objectivity

1. Procedures, mechanisms or internal guidelines demonstrating how the illegal content is accurately identified and reported (e.g. verifications or inspections carried out to submit notices), and describing the methodology for an objective assessment;
2. A correction and revision mechanism that allows adjustments in case the flagging protocols are not correctly carried out (e.g. double-check system);
3. Description of the manual and/or automated tools used to identify and verify illegal content;
4. Provide details of any commercial, financial and/or institutional relationships the entity has with the State, politicians, political parties, and how the entity ensures, in such relationship(s), the independence of the flagging activity;
5. Proof of secure data storage and protection policies and compliance with GDPR regulations.

Additional documentation:

6. Proof of previous cases where notifications have been revised and corrections have been made;
7. Process for the online platforms to report to the trusted flagger any notifications they deem to be unjustified, incorrect or incomplete;
8. Any annual report or other type of report indicating the number of notices (including the percentage of correct and incorrect notifications, adjustments, summary of disputed notifications and the handling thereof, conclusions, recommendations, etc.);
9. Reports or descriptions of previous activities or campaigns on content moderation, user protection, online security, etc.

6. Reporting obligation

Recognized trusted flaggers must publish at least once a year an easily comprehensible and detailed report.

The following documents may be provided in addition:

1. Procedure for drawing up the annual report, including who is responsible for collecting and analysing data;
2. Description of the figures and/or statistics that are used to collect the data and subsequently translated into the annual report (including the number of erroneous notifications);
3. Explanation of how data are stored, in accordance with the GDPR rules and without including personal data in the report;
4. Other similar reports;
5. Description of the technical means or systems for reporting.

ANNEX – List of Areas of Illegal Content

The list is not exhaustive and is indicative only. It reflects potential areas of illegal content across the Member States, which may constitute areas of expertise for entities applying for the status of trusted flagger.

- **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***
  - 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 behavior**
  - 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
  - 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

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

• **Offense to minors** ○ Failure to implement age-specific restrictions concerning minors ○ 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 (e.g. health) ○ Sale of non-compliant products (e.g. 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