Implementation of the Digital Services Act (DSA)

Recommendations on Trusted Flaggers

15 April 2024

Introduction

The Computer & Communications Industry Association (CCIA Europe) supports the overarching goal of the Digital Services Act (DSA)[1] to offer a secure online environment for users, including through the involvement of designated trusted flaggers under Article 22 ("Trusted Flaggers"). Trusted Flaggers are entities that have demonstrated (among other things) expertise to identify specific kinds of illegal content and properly report it to providers of online platforms to be treated as priority.

As many Digital Services Coordinators (DSCs) are currently considering the practicalities of vetting applicant Trusted Flaggers, CCIA Europe respectfully offers a set of recommendations to help make Article 22 more effective. Our recommendations are based on the extensive experience that many of our members have with operating programs prioritising content flags from specific pre-approved entities.

I. Keep the status of Trusted Flaggers meaningful
II. Put in place collaborative safeguards to protect Trusted Flaggers
III. Ensure a harmonised approach to Trusted Flaggers

I. Keep the status of Trusted Flaggers meaningful

Maintaining the integrity and effectiveness of the Trusted Flagger status is paramount in order to implement a robust process of content moderation of illegal content, as outlined in Recital 61 and Article 22 of the DSA. The process of vetting Trusted Flaggers will be a key element in ensuring this status remains meaningful.

To achieve this, applicant Trusted Flaggers should be required to demonstrate they adhere to stringent criteria; in particular that they have expertise in the relevant areas of illegal content for which they apply to be a Trusted Flagger, and also in respecting EU fundamental rights, in particular freedom of expression. The demonstrated ability to send accurate notices is an essential element of why Trusted Flaggers are trusted. The assessment of prior experience in combating the relevant category of illegal content online, capacity for scalable content identification and notification, and representation of diverse user interests should be common to all DSCs with clear metrics (e.g. harmonised benchmarks for staffing or years of experience in fighting a certain type of illegal content). Appointing organisations with proven expertise is key to avoiding compromising the efficacy of content moderation efforts and ensuring the objectives of Article 22 of the DSA are achieved.

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), available here.

Related to this, the overall number of Trusted Flaggers should be limited to prevent the dilution of the value that such a priority review system is meant to bring, and to maintain efficient processing of notices. This limitation would also allow for the representation of diverse areas of expertise, which in turn would prevent bias and ensure a comprehensive approach to content moderation.

- ➔ **Ensure all DSCs establish clear and common vetting criteria**: DSCs should define transparent standards for appointing Trusted Flaggers, scrutinising expertise in the content moderation of the relevant category of illegal content, as well as adherence to other DSA requirements. Those standards should be consistent across Member States to ensure the effective operation of Article 22 of the DSA across different types of illegal content and EU languages.
- ➔ **Limit the number of appointed Trusted Flaggers**: DSCs should limit the overall number of Trusted Flaggers to maintain quality reporting processes and the swift treatment of their notices. To ensure this, it is necessary that only industry associations, and not individual companies, may apply to be appointed as Trusted Flaggers.

The status of Trusted Flaggers may only be meaningful as long as Trusted Flaggers remain respectful of the overall architecture of the DSA. To do so, Trusted Flaggers must use the proper channels of reporting put in place by online platforms. This ensures that the prioritisation can be effective. At the same time, the other tools offered by the DSA, notably the mechanisms for users to report illegal content (Article 16), should continue to be promoted. Users should be empowered to report illegal content without depending on Trusted Flaggers.

- ➔ **Use appropriate reporting channels**: Trusted Flaggers should use the appropriate reporting channels of online platforms.
- ➔ **Enable effective user reporting of allegedly illegal content**: Users should continue to be able to report illegal content directly to providers of hosting services and not depend on Trusted Flaggers to do so.

II. Put in place collaborative safeguards to protect Trusted Flaggers

The success of the trusted flaggers mechanism will rely on cooperation to put in place the necessary safeguards to prevent abuse.

The first safeguard is based on Article 22(6) of the DSA. We recommend putting in place clear, straightforward and centralised monitoring and reporting of Trusted Flaggers to remove abusive actors. This would ensure that the information is shared quickly among the DSCs, the Commission and the online platforms. This would ensure integrity and maintain the efficiency of the Article 22 mechanism.

The second safeguard relates to the safety of Trusted Flaggers. It is important to make sure that the publishing of contact details in a database foreseen in Article 22(5) of the DSA does not lead to unintended consequences, such as spamming, impersonation or identification of individuals. To do so, the use of separate contact information should be required for Trusted Flaggers to submit notices to online platforms, and this separate contact information should be communicated in a secure manner, so that they know exactly which notices are being submitted by verified Trusted Flaggers.

- ➔ **Clear reporting of abuse**: Centralise and give guidance on the system for online platforms to report to the European Commission or DSCs of abusive actors.
- ➔ **Separate and secure contact details**: Require Trusted Flaggers to have different contact details, especially email addresses, for public communication purposes versus flagging to online platforms.

III. Ensure a harmonised approach to Trusted Flaggers

The creation of the publicly available database of names, addresses and email addresses of Trusted Flaggers foreseen by Article 22(5) should also be a priority to support the harmonised application of Article 22. The database must be put in place by the Commission as soon as possible ahead of the first appointments of Trusted Flaggers so that DSCs can upload the information from the start. Some online platforms will be able to pull from the database in real-time from an API to integrate into their notice intake systems as a signal to treat with priority. To do so, online platforms will need several weeks to integrate with this once the technical specifications are shared by the Commission. Overall, the creation of the database is an important step for accountability and transparency. This will help DSCs coordinate and limit the number of Trusted Flaggers and users to contact Trusted Flaggers.

Several aspects of the Trusted Flagger' status and mechanism need guidelines from the European Commission to ensure that the appointment and functioning of Trusted Flaggers is coherent across the 27 EU Member States, as foreseen by Article 22(8) of the DSA. These guidelines would be an appropriate vehicle to ensure that the criteria for vetting Trusted Flaggers are unified, as explained above.

- ➔ **Prioritise the Database of Trusted Flaggers**: The creation of the database gathering the identity and contact details of all appointed Trusted Flaggers is urgent and key for the good functioning of the mechanism.
- ➔ **European Guidelines to Preserve Harmonisation**: The Commission should publish guidelines setting out as granularly as possible the common standards to identify Trusted Flaggers, in particular regarding expertise, experience and objectivity of organisations.

Conclusion

CCIA Europe's recommendations on the appointment and functioning of Trusted Flaggers aim to make this essential DSA mechanism successful. By prioritising the meaningfulness of the Trusted Flagger status, preventing abuse through cooperation, and ensuring a harmonised approach across Member States, the content moderation efforts of providers of online platforms will be better supported.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

Visit ccianet.org/hub/europe/ or x.com/CCIAeurope to learn more.

For more information, please contact:

CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org