WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

POSITION PAPER

on the Commission Draft Guidelines on the trusted flagger mechanism under Article 22 of Regulation (EU) 2022/2065

Cologne/Berlin, 6 July 2026

On 29 May 2026, the European Commission published its draft guidelines on the trusted flagger mechanism under Article 22 of Regulation (EU) 2022/2065 (Digital Services Act – DSA) for a targeted public consultation. The guidelines aim to assist and to provide further interpretative guidance for the Digital Services Coordinators (DSCs) in the member states, providers of online platforms and entities applying for or acting as trusted flagger under the DSA.

eco – Association of the Internet Industry (eco) welcomes the opportunity to comment on the draft guidelines. The following feedback and suggestions are based on the experience of eco's members as well as eco's own experience as the operator of a hotline for reporting illegal content online (eco Complaints Office).

eco members include companies from among the whole value chain of the internet.

eco has been operating its hotline for 30 years dedicated to combatting illegal and youth-endangering content. The eco Complaints Office serves as a point of contact for users, assesses reported content based on the legal framework in Germany and, in case of identified illegal content, notifies providers of hosting services or online platforms.

Thus, there is both: On the one hand experience and expertise in receiving notifications about illegal content or online threats and report handling, and on the other hand, expertise in detecting, investigating, and reporting of online threats.

eco welcomes the Commission Draft Guidelines. They are an important tool and essential guidance for a consistent and harmonised implementation of the Trusted Flagger scheme under the DSA.

With regard to the draft guidelines, eco would like to make a few points related to:

- Awarding the trusted flagger status
- Submission and processing of notices
- Safeguarding the integrity of the trusted flagger status

1. Awarding the trusted flagger status

An essential part of the draft guidelines is related to awarding the trusted flagger status. While in principle, the draft guidelines are appropriate to provide clarity and to assist both, the national DSCs and the entities applying for the trusted flagger status, eco would like to point out the following:

- Eligible entities

Paragraphs 29 to 32 (d) are addressing the issue of eligible entities which could be: (i) public in nature, (ii) semi-public, (iii) non-governmental organisations, or (iv) private entities.

With regards to eligible private entities, eco recommends amending the guidelines, particularly paragraphs 32(b) and 32(c). eco would like to point out, that it would be from an industry point of view helpful to clarify, that all applicants should be treated in general equally and that aspects including commercial or other interests interfering with the activities of the trusted flagger should be the limiting aspects (and not the fact of having commercial or other interests themselves) in order to allow for specialized service providers to take part in the flagging process without undue scrutiny due to other commercial activities.

Submitting notices on behalf of third parties is a standard, legitimate function in the internet industry, e.g. with regard to cyber security, and is not meaningfully different in public interest terms from other entities submitting notices on behalf of third parties, e.g. in the area of cyberviolence. Therefore, eco suggests rephrasing the wording of these articles.

More generally speaking, it is important that no sector is de facto excluded per se from the outset. Ultimately, the decisive factor must be whether the conditions laid down in Article 22 (2) DSA are met. None of these conditions exclude a specific sector, commercial entities or business models based on client representation.

As regards the possibility for public bodies to apply for trusted flagger status, the fact that departments of national authorities with powers to issue legally binding illegal content orders could also be eligible for trusted flagger status creates significant independence and administrative overreach concerns. Even if the department acting as trusted flagger is not empowered to issue orders to act against illegal content, it is not clear how distinguishing between a non-binding notice and a legally binding order would be implemented in practice.

- Conditions for the trusted flagger status

Paragraphs 33 to 43 are addressing the conditions for the trusted flagger status: expertise and competence in detecting, identifying and notifying illegal content, independence from online platform providers, and submitting notices diligently, accurately and objectively.

With regard to “independence”, eco welcomes that the paragraphs related to this criterion (particularly 38 and 39, but also 43 and the included example) put a clear spotlight on the relevance of neutral and objective decision-making processes. The same counts for the clear statement that any cooperation or financial contribution shall not automatically lead to the assumption that the applying entity is not independent.

To give an example: Looking at the well-established hotlines of the INHOPE network and Safer Internet Centers in the EU Member States, these hotlines often are trusted partners on a voluntary basis for providers of online platforms and other intermediary services for years. They demonstrated their competence and

knowledge in objectively identifying and notifying illegal online content over the last up to 30 years. Thus, various providers of hosting services and online platforms granted them a trustful status.

The hotlines' experience makes them a predestined candidate for applying for the trusted flagger status under the DSA. It would be detrimental to the ecosystem and send a negative signal regarding the fight against illegal content online, if any cooperation with platform providers or any financial contribution for running a hotline would automatically deem hotlines not to be independent and consequently would be a showstopper for awarding hotlines the trusted flagger status under the DSA.

The neutral assessment and independent decision-making process when detecting, identifying and notifying illegal content is the key criterion. In principle, this is already made clear in the draft guidelines. Nevertheless, eco suggests emphasising this even more clearly by explicitly stating this premise at the beginning of the section/ these paragraphs as well.

With regard to the accuracy criterion and applications of private entities, the draft guidelines state that DSCs should apply particular scrutiny to those entities that don't have public interest mission and where private interests, and in particular commercial considerations, may reasonably be expected to impact their trusted flagger activity. In these cases, DSCs may subject such entities to a higher degree of scrutiny, including for example as regards the accuracy rate in their notices compared to other entities in the same designated area of expertise.

In this regard, eco would like to make the following points for consideration.

On the one hand, commercial interests or acting on behalf of a third party must not de facto or automatically result in less accuracy when notifying illegal content or online threats. To give an example, specialized service providers that submit notices on online threats such as phishing on behalf of enterprise clients usually have an operational interest to align with accurate, well-substantiated notices: a high false-positive rate damages client relationships, undermines the firm's credibility with platforms, and risks status revocation under Article 22(7).

On the other hand, depending on the specific application in question, it could be appropriate and reasonable for the DSC that the scrutiny includes a review of not only accuracy but also proportionality of the notices of alleged illegal content to ensure that impact to legal content isn't disproportional. It can also be important to assess whether the applying entity usually sends notices to the most appropriate provider who can address the issue and not the most convenient one.

- General remarks on the application process

On a more general note, with regard to the application process, eco realized that processing timelines vary widely: some DSCs have awarded multiple certifications within months of application; others have significant backlogs with no publicly stated processing timeline. The draft guidelines acknowledge at paragraph 57 that applications should be assessed swiftly without being forced to process applications in the order of submission in order to allow applications to be prioritized that cover

underrepresented areas of expertise. This is welcome guidance; however, applicants might need to have a reasonable planning horizon. Thus, swift feedback of the DSC to the applicant on the forthcoming procedure, potentially missing documents and an estimated timeline would be helpful.

On another note, the DSA and the guidelines allow organizations that represent private interest (e.g. rightsholders interest) to be trusted flaggers. When processing their application, it could be reasonable to pay particular attention to sufficient transparency of the entity about whose interests are represented. Transparency on the represented interests might also be reasonable and helpful when it comes to the publication of the awarded trusted flagger status.

With regard to novel applicant types, particularly commercial entities and other specialized service providers e.g. cybersecurity, eco suggests considering a cross-DSC peer review process amending the standard review process since established practice is still developing. A peer review process could prevent divergent national interpretations of the same eligibility criteria leading to inconsistent outcomes across member states.

2. Submission and processing of notices

The section on the submission and processing of notices covers various aspects and obligations for providers of online platforms including the onboarding of trusted flaggers, the submission and processing of notices by trusted flaggers as well as prioritisation of reports. (Paragraphs 74 to 90)

- Intake of trusted flagger reports

With regard to offering contact points and intake channels for the submission of notices by trusted flaggers (paragraph 76), eco welcomes the statement in paragraph 126 of the draft guidelines that providers of online platforms can choose to open these reporting channels for other trusted partners as part of their voluntary cooperation, as long as this does not hinder the priority which is to be given to notices from trusted flaggers under the DSA. This reflects the existing of trusted partners on a voluntary basis and their impact in the fight against illegal content online. In addition, it gives the platforms providers the necessary flexibility to offer one reporting channel for both, trusted flaggers under the DSA and trusted partners on a voluntary basis, or to choose offering different reporting channels – whichever suits best for the specific online platform provider.

At the same time, eco is concerned by statements in the guidelines suggesting that platforms must provide “dedicated channels” for trusted flagger reporting, given Article 22 DSA makes clear that the same intake mechanism as under Article 16 DSA may be used.

eco also notes that the guidelines recommend that notices submitted by trusted flaggers be processed with an additional verification step; and that providers of online platforms grant trusted flaggers access to an API to facilitate the submission of notices and enable standardised retrieval of information. These

recommendations find no basis in the DSA text and would impose additional, significant compliance burdens on online platforms.

Finally, eco objects to the recommendation that providers of online platforms use the types of illegal content in the transparency reporting template when taking the technical and organisational measures to which Article 22 refers. This is not required by the DSA and would be practically infeasible and/or not user-friendly given the number of categories in the transparency reporting template.

- Prioritisation

Even in case of notices submitted by trusted flaggers, there might be a need for prioritisation for the receiving online platform provider. eco welcomes that the draft guidelines acknowledge this circumstance.

With regard to prioritisation, the severity of the content notified or urgency are the essential criteria. Thus, eco suggests reconsidering paragraph 89 to avoid misinterpretation. For instance, the paragraph could slightly be redrafted by stating that the provider should "in principle/ generally ensure balance in the time needed for taking a decision across different types of content so that in general notices in each area of expertise may benefit". This would make clear that the balance and benefit for each area of expertise shall be the general rule, but that there might be scenarios where platform providers have to and are allowed to give several times priority to the severity and urgency of a content notified.

3. Safeguarding the integrity of the trusted flagger status

Safeguarding the integrity of the trusted flagger status by providing the opportunity to suspend and revoke this status by the awarding DSC is important for a reliable and trustworthy trusted flagger scheme under the DSA.

With regard to communicating insufficient, inaccurate or inadequate substantiated reporting of trusted flaggers to the DSCs, eco suggests reconsidering paragraph 100 which addresses this issue. In the current version, the platform provider has to undertake a detailed assessment. The provisions for the platform providers should be simplified.

When it comes to safeguarding the integrity of the trusted flagger status the findings and observations of the online platform providers play an important role. Consequently, it is essential that they report any suspicions of significant insufficient, inaccurate or inadequate substantiated notices to the responsible DSC. In practice, a platform provider will inevitably undertake internal checks, weights and comparisons in order to determine whether a trusted flagger submits a significant number of insufficient, inaccurate or inadequate substantiated notices.

However, online platform providers should not be forced to undertake a detailed assessment or be bound by specific evidence points they need to provide in every case. The detailed assessment actually should be part of the DSCs investigation and assessment. For the provider of online platforms, it must be sufficient to submit substantial evidence to the DSC.

4. Conclusion

eco broadly welcomes the Commission Draft Guidelines. Some amendments concerning (i) eligible entities, (ii) the independence and accuracy criteria, (iii) the evaluation process of the DSCs, (iv) the operationalisation of reports, and (v) the reporting of a significant number of insufficient, inaccurate or inadequate substantiated trusted flagger notices to the DSC would be necessary to create even more clarity and assistance.

About eco: With approximately 1,000 member companies, eco (international.eco.de) is the leading Association of the Internet Industry in Europe. Since 1995, eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of its members in politics and international forums. eco has offices based in Cologne, Berlin and Brussels. In its work, eco primarily advocates for a high-performance, reliable and trustworthy ecosystem of digital infrastructures and services.