Position Paper on the Digital Services Act's (DSA) Implementation

Strengthening the European Commission's guidelines for trusted flaggers

July 2026

The Computer & Communications Industry Association (CCIA Europe) welcomes the opportunity to provide feedback on the European Commission's draft guidelines on the trusted-flagger mechanism under Article 22 of the Digital Services Act (DSA).[1] The Association respectfully submits the nine recommendations set out below.

I. Upholding the scope of the Digital Services Act

The Commission's guidelines must remain strictly within the confines of Article 22 DSA. Expanding the regulatory scope through secondary guidance would undermine legal certainty and impose disproportionate administrative burdens on intermediary services.

Recommendations:

1. Maintain platform autonomy over intake mechanisms
2. Limit transparency and disclosure mandates strictly to the DSA text
3. Prevent extra-legal oversight requirements not grounded in the DSA

II. Guaranteeing strict independence of trusted flaggers

The integrity of the trusted-flagger framework depends entirely on the strict impartiality of designated entities. Hence, the guidelines must establish rigorous safeguards to prevent the mechanism from being co-opted, while ensuring that fundamental rights remain protected.

Recommendations:

4. Mitigate risks of bias and commercial motivation
5. Provide pragmatic criteria for assessing financial independence
6. Exclude public bodies and state authorities from trusted-flagger status

III. Ensuring workable and harmonised frameworks

To prevent system fragmentation and operational paralysis, procedures governing trusted flaggers must be streamlined, practical, and uniformly applied across the Single Market – all while respecting the contractual freedom of digital services.

Recommendations:

7. Streamline the onboarding and designation process to prevent overload
8. Align prioritisation and trusted-flagger obligations with operational realities
9. Protect platforms' freedom to handle misuse and voluntary partnerships

[1] European Commission, 'Targeted public consultation on the Guidelines on the trusted flagger mechanism under Article 22 of Regulation (EU) 2022/2065 (Digital Services Act)', available here.

Introduction

The Computer & Communications Industry Association (CCIA Europe) welcomes the draft guidelines' emphasis on funding transparency, operational independence, accountability, and the clear statement that trusted flaggers do not decide whether content should be removed. Nevertheless, we believe that the Commission's final set of guidelines should prioritise legal clarity and operational feasibility, rather than expanding the Regulation's scope or altering established content-moderation dynamics.

Indeed, the existing Digital Services Act (DSA)[2] framework already provides a strong, delicately balanced foundation for tackling illegal content online. Based on the draft guidelines presented by the European Commission, CCIA Europe has identified several areas where they go beyond the DSA text as well as instances that require further clarification.

To create a workable system without undermining the autonomy of online platforms, the Commission should simplify the procedures currently proposed in the draft and guarantee the strict neutrality of trusted flaggers. CCIA Europe also stresses that the effectiveness of the trusted flagger mechanism must be measured not only by the speed with which genuinely illegal content is addressed, but also by the safeguards that protect legitimate businesses from wrongful removal of legitimate content.

Over-removal driven by high-volume or insufficiently substantiated notices imposes real and disproportionate harm on good-faith providers and their European users. A workable mechanism must therefore balance prioritisation with accuracy, substantiation, and meaningful redress.

To that end, CCIA Europe submits nine recommendations aimed at safeguarding the efficiency and integrity of the trusted flagger mechanism, grouped around three overarching themes:

1. Upholding the scope of the Digital Services Act
2. Guaranteeing strict independence of trusted flaggers
3. Ensuring workable and harmonised frameworks

The Association stands ready to support the Commission in achieving these objectives.

[2] Regulation (EU) 2022/2065 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available here.

I. Upholding the scope of the Digital Services Act

The Commission's guidelines must remain strictly within the confines of Article 22 DSA. Expanding the regulatory scope through secondary guidance would undermine legal certainty and impose disproportionate administrative burdens on intermediary services.

1. Maintain platform autonomy over intake mechanisms

While the draft guidelines assert that platforms must develop "dedicated channels" to process trusted-flagger reports, Article 22 DSA is unambiguous in stating that these notices are to be submitted via the existing notice and action mechanisms established under Article 16 DSA. Imposing a mandate for a separate mechanism creates unnecessary duplication and disproportionate compliance costs. CCIA Europe proposes that platforms retain the autonomy to integrate trusted-flagger prioritisation within their current Article 16 DSA architecture, ensuring efficiency without mandated structural overhauls.

2. Limit transparency and disclosure mandates strictly to the DSA text

The draft guidelines, in paragraph 12, suggest that providers of hosting services must declare the involvement of a trusted flagger in the Statement of Reasons provided to users whose content is restricted. However, Article 17 DSA, which actually deals with the Statement of Reasons, contains no such requirement.

Furthermore, instructing providers of hosting services and Digital Services Coordinators (DSCs) to adopt the specific classifications from the transparency reporting templates for their intake forms and expertise designations oversteps the legislative mandate of Articles 16 and 22 DSA.

CCIA Europe calls on the Commission to remove both of these information requirements to avoid generating administrative friction. The Association also firmly rejects paragraph 128, which mandates platforms to publicly disclose voluntary cooperation with trusted flaggers on their interfaces to maintain public trust and accountability. There is no disclosure requirement in the DSA and staying within the letter of the law is required to guarantee legal certainty for online platforms.

3. Prevent extra-legal oversight requirements not grounded in the DSA

The Commission's draft guidelines introduce additional technical and procedural stipulations that lack a legal basis in the text of the DSA and threaten the effective functioning of the mechanism. Mandating advanced technical measures, such as two-step verification systems, secure digital certification, the provision of application programming interfaces (APIs) for trusted flaggers, or requiring issues to be resolved before reporting misuse constitutes regulatory overreach.

Additionally, there is no disclosure requirement as part of the DSA mandating platforms to publicly disclose these voluntary, commercial relationships on their interfaces, nor any obligation for platforms to ensure balance in the time needed for taking a decision across all illegal content types. Further recommendations on these extra-legal oversight requirements are included in section III, specifically in recommendations 7 and 9.

II. Guaranteeing strict independence of trusted flaggers

The integrity of the trusted-flagger framework depends entirely on the strict impartiality of designated entities. Hence, the guidelines must establish rigorous safeguards to prevent the mechanism from being co-opted, while ensuring that fundamental rights remain protected.

4. Mitigate risks of bias and commercial motivation

Under Article 22 DSA, independence is a strict, mandatory requirement to be certified as a trusted flagger. Recognising that entities with commercial interests may apply for trusted-flagger status, the guidelines should ensure that any action undertaken by a trusted flagger is grounded in supporting compliance with the DSA.

To that end, paragraph 32(b) should be revised so that DSCs "should" or "must" (not merely "may") subject entities with commercial interests to a higher degree of scrutiny when assessing trusted-flagger applications and activities. This will protect the mechanism from being weaponised to serve commercial objectives or political views.

CCIA Europe calls for the introduction of mandatory periodic reviews and renewal requirements of the trusted-flagger status, rather than granting it indefinitely. This would ensure compliance with the independence and objectivity requirements. Stronger safeguards should also be considered to prevent large umbrella organisations from exploiting the system across multiple jurisdictions or policy domains. The guidelines should also define in much greater detail what constitutes sufficient expertise for designation under Article 22(2)(a) DSA.

To complement existing rules and ensure an unbiased system, a mechanism could be established allowing online platforms to report trusted flaggers who repeatedly target them while ignoring identical content elsewhere. This would reinforce confidence in the system's fairness and objectivity.

5. Provide pragmatic criteria for assessing financial independence

The current draft, in paragraph 30, lacks concrete methodologies for DSCs to practically assess conflicts of interest. CCIA Europe welcomes the clarification in paragraph 39 that financial support from online platforms does not inherently compromise the independence of an entity applying for trusted-flagger status. However, we believe that DSCs require concrete good practice examples to guide their evaluations.

Paragraph 36, which lists what DSCs should take into account in order to verify the condition of independence, should provide a flexible, case-by-case assessment model. Indeed, entities may already participate in existing platform priority-flagger programmes governed by strict non-disclosure agreements (NDAs), preventing them from disclosing this information.

CCIA Europe encourages the European Commission to clarify in paragraph 40 that feedback through recommendation letters regarding an applicant's operational track record must remain entirely optional for platforms.

6. Exclude public bodies and state authorities from trusted-flagger status

The draft guidelines, in paragraph 31, establish that: 1) national authorities not empowered for the adoption of orders to act against illegal content; or 2) departments of national authorities empowered for the adoption of such orders with sufficient management and operational autonomy should be eligible for trusted-flagger status.

CCIA Europe opposes the designation of public bodies or departments of national authorities as trusted flaggers. This threatens the independence of the mechanism and contradicts the core DSA requirement that trusted flaggers must operate with a high degree of freedom from state or any other influence that may affect their objectivity. Furthermore, CCIA Members consider that this blurring of the line between non-binding notices and mandatory legal orders risks causing significant procedural confusion.

III. Ensuring workable and harmonised frameworks

To prevent system fragmentation and operational paralysis, procedures governing trusted flaggers must be streamlined, practical, and uniformly applied across the Single Market – all while respecting the contractual freedom of digital services.

7. Streamline the onboarding and designation process to prevent overload

To ensure the trusted-flagger system remains functional despite a high volume of participants, CCIA Europe suggests that the final guidelines explicitly limit participation by individuals acting with commercial interests. Instead, they should prioritise collective or representative bodies that satisfy the required scrutiny of commercial considerations, especially for the enforcement of intellectual property rights.

Individual rightsholders should only be granted trusted-flagger status in limited cases where strong accuracy, objectivity, conflict-of-interest, and volume-management safeguards are met. This will help limit the overall number of trusted flaggers, prevent system overload, and the dilution of the value that such a priority review system is meant to bring, and maintain efficient processing of notices. This would also help prevent bias and ensure a comprehensive approach to content moderation.

In the context of the onboarding process, platforms are requested by the guidelines in paragraph 72 to designate a single electronic point of contact easily identifiable and adequately staffed to ensure responsiveness and a smooth onboarding process. The Commission should explicitly recognise the use of established points of contact under Article 11 DSA, instead of developing redundant interfaces. We also urge the Commission to clarify that platforms are only expected to process notices under the Article 22 DSA regime after the central database has officially been updated to confirm the flagger's status.

Furthermore, trusted flaggers must be explicitly held responsible for directing their notices to the specific provider that controls and is responsible for the content, rather than targeting broad, secondary infrastructure such as app stores.

CCIA Europe also believes that the identity-verification requirements for trusted flaggers' onboarding and submission of notices outlined in paragraphs 70 and 78 – which suggest

multiple authentication layers and specific methods like secure digital certification or two-step verification – are excessively prescriptive. Rather than mandating particular technical layers or methods, the guidelines should allow platforms the flexibility to implement verification processes that are appropriate and proportionate to their specific systems.

What is more, the guidelines assume that a formal onboarding procedure is essential in every instance. CCIA Members believe this requirement should be more flexible. In cases where platforms currently permit trusted flaggers to self-identify through existing reporting forms at the time of submission, a separate onboarding layer offers no additional value and creates redundant administrative steps. Hence, the guidelines should acknowledge that formal onboarding should only be mandated when it provides a genuine improvement to the submission workflow.

CCIA Europe welcomes the invitation to DSCs to refer to the guidelines when implementing the mechanism in Article 22 DSA and awarding the status of trusted flaggers. However, we believe that DSCs must adhere strictly to them and avoid drafting divergent national rules, which would undermine the application of the mechanism and fragment the Single Market.

8. Align prioritisation and trusted-flagger obligations with operational realities

Paragraph 84 establishes that prioritisation of notices should be driven by the severity of the illegal content notified, where accelerated processing is desired to minimise harm, in particular where notices relate to physical harm or threats to safety, as well as the virality of the content and other time-sensitive factors. While severe threats to life or the safety of persons naturally command immediate attention, this paragraph risks creating an unworkable paradigm by demanding concurrent prioritisation across an ever-expanding array of granular transparency categories. If platforms are forced to prioritise everything simultaneously, the concept of prioritisation is entirely neutralised.

Against this background, given the rapidly expanding trusted-flagger ecosystem (currently exceeding 70 entities), and the detailed requirements set out in the draft guidelines, the deployment of automated means is not merely advisable, but necessary to meet the obligation to process notices "without undue delay" as required by Article 22(1) DSA. The Commission's acknowledgment in paragraph 87 that "available technologies" may be appropriate is welcome. Nevertheless, the final guidelines should develop this aspect further and explicitly recognise that automation is essential to operationalise the mechanism at scale.

Furthermore, the draft's expectation that platforms "ensure balance in the time needed for taking a decision" (see paragraph 89) across all illegal content types imposes an unworkable secondary layer of triage not found in the DSA. CCIA Europe also insists that performance metrics regarding processing speed must rely on 'median' rather than 'average' times – formally acknowledging that legally complex notices inherently require extended review periods.

To ensure a functional mechanism, the guidelines should also clarify that trusted flaggers must only report content illegal under their home Member State's laws, unless based on

directly applicable Union law. A national DSC cannot accurately assess an entity's expertise in the diverse national laws and judicial interpretations of other jurisdictions.

Finally, the guidelines should clarify that notices outside a trusted flagger's certified expertise must be submitted via the standard Article 16 DSA mechanism, rather than the priority channel. Article 22 DSA grants trusted-flagger status based on "particular expertise," which justifies expedited processing. Allowing out-of-scope notices into the priority pathway undermines this presumption, adds complexity, and creates false expectations for enhanced treatment. Article 16 DSA remains the appropriate channel for such submissions.

9. Protect platforms' freedom to handle misuse and voluntary partnerships

Article 22 of the DSA mandates priority processing, not automatic content removal. This distinction is particularly important for legitimate businesses that could become caught up in erroneous or contested notices. The guidelines should therefore reinforce safeguards ensuring that prioritised notices remain accurate and substantiated, and that affected users retain effective and timely means of redress.

Requiring platforms to provide retroactive access to data concerning notices from trusted flaggers through distinct channels – specifically APIs as suggested in paragraphs 79-88 – is unfounded. Given that most of this data is already accessible via standard Article 16 DSA notice processing, these mandates are seen as disproportionate. The proposed requirements for information also go beyond the rules applicable to platforms under Article 16 DSA. While Article 16(6) DSA mandates that platforms inform trusted flaggers of decisions regarding their notices, it does not require platforms to record and communicate the precise time at which action was taken.

Moreover, the suggestion in paragraph 103 that providers of online platforms must consult with trusted flaggers to resolve disagreements before reporting any misuse to the DSC to remedy disagreements over the quality of notices is simply not required by Article 22 DSA. These extra-legal requirements undermine the independent oversight role of the platforms and should be removed.

CCIA Europe also considers that the revocation of an entity's trusted-flagger status by a DSC should not trigger regulatory pressure on platforms to reassess their separate, voluntary cooperation arrangements with that entity, as currently set out in paragraph 123. Paragraph 67, which states that providers of online platforms should regularly consult the Trusted Flaggers Database and use automated methods to receive updates from the machine-readable database, is unnecessarily prescriptive.

Platforms should retain the discretion to choose their own methods for monitoring database updates, as long as those methods remain effective. To simplify tracking, consideration should be given to introducing periodic change reports that document when flaggers are added, removed, or have their information modified. Finally, as already stressed in our second recommendation, platforms should not be required to provide public disclosure of their voluntary partnerships with trusted flaggers within their user interfaces.

Conclusion

Secondary guidelines should serve to clarify existing EU legislation, not expand its reach. Using the trusted-flagger guidelines to broaden the Digital Services Act's scope would be inappropriate and unjustified. Rather than introducing additional prescriptive obligations that were rejected during the legislative process, the European Commission should focus on ensuring that the trusted-flagger mechanism is legally sound, strictly independent, and operationally viable.

We therefore urge the Commission to revise the current guidelines to safeguard platforms' structural autonomy, strictly exclude state authorities from the flagging process, and eliminate bureaucratic overlaps. By adhering to these principles, the Commission can ensure a harmonised and effective approach to tackling illegal content across the European Union.

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.eu, x.com/CCIAeurope, or linkedin.com/showcase/cciaeurope to learn more.

For more information, please contact:
CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org