

INACH

Bringing the Online In Line with Human Rights

Advocacy and Policy Development Forum 2026

Compiled by
INACH + CEJI
2026

Table of Contents

INTERNATIONAL NETWORK AGAINST CYBER HATE – INACH **2**

INTRODUCTION **3**

PANEL OVERVIEW **3**

LEVERAGING THE DSA: CIVIL SOCIETY PATHWAYS TO COUNTER ONLINE HATE 3

TRUSTED FLAGGERS IN PRACTICE: EXPERIENCES, CHALLENGES AND CROSS-DOMAIN INSIGHTS UNDER THE DSA 6

ROUNDTABLE SESSION| COLLECTIVE ADVOCACY: OPPORTUNITIES, GAPS AND STRATEGIC DIRECTIONS **9**

RECOMMENDATIONS **10**

International Network Against Cyber Hate – INACH

INACH was founded in 2002 to use intervention and other preventive strategies against cyber hate. The member organisations are united in a systematic fight against cyber hate, for example as complaints offices, monitoring offices or online help desks. In their respective countries, they provide important contacts for politicians, internet providers, educational institutions, and users.

Funding for INACH is provided by its members, the European Commission, the BPB and other donors. The International Network Against Cyber Hate (INACH) unites multiple organizations from the EU, Africa, Albania, Israel, North Macedonia, Russia, South America, and the United Kingdom. While starting as a network of online complaints offices, INACH today pursues a multi-dimensional approach of educational and preventive strategies.

This publication has been produced with the financial support of the Citizens, Equality, Rights and Values (CERV) Programme of the European Union. The contents of this publication are the sole responsibility of the International Network Against Cyber Hate and can in no way be taken to reflect the views of the European Commission.

Supported by the Citizens, Equality, Rights and Values (CERV) Programme of the European Union

Introduction

The Advocacy and Policy Development Forum took place on 5 March 2026 in Brussels. The event was attended by about 30 representatives of CSOs, the European Commission, the EU Agency for Fundamental Rights, Coimisiún na Meán and the Appeals Center Europe. The agenda included two panels, a roundtable brainstorming session and a workshop by Hateaid.

Panel Overview

In the following section you will find an overview and discussion points from our two panels.

Panel 1

Leveraging the DSA: Civil Society Pathways to Counter Online Hate.

With Carl van der Maelen (DG CONNECT), David Reichel (EU Agency for Fundamental Rights), Niamh Hanafin (Coimisiún na Meán),The Irish DSC, and Tommaso Chiamparino (DG JUSTICE).

Panel 2

Trusted Flaggers in Practice: Experiences, Challenges and Cross-Domain Insights Under the DSA

With Fiorentina Azizi-Hacker (ZARA), Carmen Weyer (Bee Secure / KJT), Henk van Kempen (MOD), and Audrey Koulidiati (LICRA).

Leveraging the DSA: Civil Society Pathways to Counter Online Hate

The DSA places significant emphasis on the role of Civil Society Organizations (CSOs) within the broader response system of digital governance and platform accountability. The DSA regulation includes numerous commitments that underline the importance of

multistakeholder engagement in the development, implementation, and oversight of platforms' policies.

A notable example of this approach was the multistakeholder meeting held in June 2025 in Dublin with Monitoring Organisations of the Code of Conduct on Illegal Hate Speech Online, which demonstrated how collaboration between regulators, platforms, and civil society has the potential to strengthen content moderation processes. Such initiatives illustrate how CSOs contribute valuable expertise and independent monitoring capacities that help ensure platforms meet their obligations under the DSA.

Civil society monitoring plays a crucial role in identifying emerging trends and evolving digital harms. Through research, monitoring exercises, and reporting, CSOs help hold platforms accountable for their commitments under the regulation. Their work often provides early warnings about harmful trends and helps highlight gaps in platform responses.

However, there are increasing concerns about the imbalance between expectations placed on CSOs and the resources available to them. Organizations working on issues such as online hate speech and harmful content are facing growing risks, including harassment, defamation campaigns, and legal threats. In some cases, these risks have escalated to serious incidents, such as attacks against organizations like HateAid. As a result, there is a growing call for stronger support mechanisms from European to national levels, including coordination between regulators to protect civil society actors carrying out this essential work.

From the perspective of the European Union Agency for Fundamental Rights (FRA), there is a clear mandate to promote dialogue between civil society and regulators. One of FRA's roles is to serve as a bridge between civil society organizations and regulatory bodies, ensuring that CSO perspectives are reflected in regulatory discussions and implementation processes. Within the context of the DSA, FRA has highlighted the importance of examining the role of civil society in content moderation and is considering publishing further analysis or reports on this topic.

Digital Services Coordinators (DSCs) have also emphasized that CSOs are a critical stakeholder group explicitly recognized within the DSA framework. Despite the rigid legal

structures that govern regulatory implementation, engagement with civil society has become an important part of DSA enforcement. This engagement occurs across several areas, including complaint handling mechanisms, user support structures, and supervisory processes that benefit from civil society input.

Regulators have observed that CSOs often provide important contextual information that platforms and authorities may otherwise lack. For example, in interactions between DSCs and major service providers, civil society organizations have been able to contribute nuanced insights into specific complaints and emerging trends, which helps regulators better understand the societal implications of platform practices.

At the same time, several challenges remain. One of the most pressing issues concerns the ability of regulators and CSOs to address emerging trends. Many organizations lack sufficient resources to monitor rapidly evolving online harms or to respond to new digital trends as they arise. In response to these constraints, there has been a noticeable increase in CSOs pursuing litigation pathways, which sometimes produce faster results than the regulatory mechanisms available under the DSA.

To strengthen collaboration, new initiatives are currently being developed to formalize civil society engagement. One such initiative involves the creation of an online application process for CSOs interested in contributing to DSA-related work. The application would gather information on organizations' expertise, research publications, and their envisioned role within the DSA response system. Within Working Group 2 of the DSA Board, efforts are underway to expand outreach and develop more structured forms of cooperation with civil society actors.

The European Commission has also acknowledged the funding challenges faced by CSOs. As part of its obligations under the DSA, the Commission must establish structured engagement with a large number of organizations—approximately 900 civil society actors—that contribute input to annual reports and policy discussions. However, there remains a limited number of CSOs that specialize exclusively in digital issues. Increasingly, traditional civil society organizations are encountering digital dimensions in their work, such as online harassment, misinformation, and digital discrimination. The Commission

is therefore seeking to strengthen cooperation between regulators and civil society and is planning to launch a public consultation to support this process.

Data access remains another major challenge. Both regulators and CSOs report that collecting meaningful data from large online platforms remains difficult. For example, obtaining data from companies such as Meta continues to present practical and procedural obstacles, limiting the ability of civil society monitoring and regulators oversight.

At the national level, new initiatives are also emerging. In Ireland, for instance, a policy team is currently working with civil society organizations and is preparing to launch a pilot project that will allow CSOs to submit insights, research findings, and data related to digital harms directly to the Digital Services Coordinator, Coimisiún na Meán (CNAM).

Finally, broader EU policy developments are reinforcing the importance of civil society participation. In November 2025, the European Commission adopted the EU Strategy for Civil Society, which emphasizes the essential role that civil society plays in safeguarding democratic values and fundamental rights. This initiative aims to renew the EU's commitment to protecting the work of CSOs and to create new opportunities for supporting civil society engagement, including in the field of digital governance.

Trusted Flaggers in Practice: Experiences, Challenges and Cross-Domain Insights Under the DSA

The implementation of the Trusted Flagger (TF) system under the DSA requires an approach that is process-oriented, adaptive, and reflective. Establishing effective Trusted Flagger mechanisms depends on clearly defining the mandate, scope, and national legal basis for the role. Transparency is also essential: Trusted Flaggers need to operate within frameworks that include public reporting obligations and clear communication about their activities and responsibilities.

Ensuring the independence of Trusted Flaggers is a fundamental requirement under the DSA. For example, when organizations cooperate with government institutions—such as ministries responsible for education or digital policy—it is essential to establish clear

boundaries between political actors, regulators, and platforms. Governance structures must clearly separate funding arrangements from operational decision-making to safeguard the credibility and independence of the reporting process. Additionally, legal mandates should be clearly defined to prevent ambiguity and to avoid the risk of over-notification or misuse of the reporting system.

For many organizations, particularly smaller NGOs, the process of becoming certified as a Trusted Flagger has been one of the most significant hurdles. Questions around what constitutes "independence" under the DSA remain difficult to interpret in practice. Some organizations, such as ZARA in Austria, have extensive experience in monitoring and reporting illegal content, yet still faced lengthy and complex certification processes.

Even after certification, onboarding has not always been smooth. In some cases, it took significant time for the organization's information to be listed on official EC websites, and even longer for large online platforms to initiate contact. Some platforms have not contacted certified Trusted Flaggers at all. This indicates a need for clearer procedures governing how Trusted Flaggers are onboarded by platforms, including defined timelines and communication protocols.

Reporting processes differ widely across platforms. While some large platforms have relatively structured systems for Trusted Flaggers, smaller platforms often lack accessible or consistent reporting channels, making it difficult to submit reports effectively.

Ethical and reputational challenges also arise. Trusted Flaggers are sometimes perceived by the public as "censors," which can lead to backlash against organizations and individuals involved in reporting content. This perception has increasingly created an environment where civil society actors fear reputational attacks, legal threats, or harassment for continuing their reporting activities. As a result, some organizations are now preparing legal and litigation strategies to respond to potential attacks.

Several legal issues have emerged regarding the responsibilities of Trusted Flaggers. One example concerns the handling of child sexual abuse material (CSAM). In Austria, for instance, it is illegal for Trusted Flaggers to possess or even view such material. This raises practical questions when such content is inadvertently sent to reporting organizations. To address this issue, agreements have been established in which the material is

immediately forwarded to the relevant authorities and then deleted. Other jurisdictional questions remain unresolved. For example: What responsibility do Trusted Flaggers have for content that originates outside their country but remains accessible domestically?

The legitimacy of the Trusted Flagger system depends heavily on the credibility of its analysis and its alignment with EU legal frameworks. While many organizations collect large amounts of data, there is a need to improve analytical methodologies. Simply identifying the presence of hate speech is not sufficient; Trusted Flaggers must also identify patterns, trends, and systemic issues across platforms.

In addition, Trusted Flaggers should develop a deeper understanding of how platforms operate beyond the reporting interface. Knowledge of moderation systems, recommendation algorithms, and platform governance structures is essential for building credibility and improving the effectiveness of reporting. Developing this expertise can also strengthen cross-border collaboration between organizations.

One common metric used to evaluate the effectiveness of Trusted Flaggers is the removal rate of illegal content following reports. However, the implementation of certain DSA provisions remains uneven in practice. Platforms are required to make reporting accessible, yet in some cases the reporting mechanisms do not comply with accessibility standards.

There are also inconsistencies in how organizations must explain or contextualize their reports to platforms. Character limits in reporting forms often prevent organizations from providing sufficient context, while platforms may simultaneously reject reports for lacking adequate information.

Strengthening networks between Trusted Flaggers is widely recognized as essential. Collaboration can help build shared methodologies, strengthen professional standards, and improve collective expertise. There is a need for clearer guidelines and more structured cooperation among Trusted Flaggers across countries.

Such collaboration could include:

- Shared methodological frameworks
- Capacity-building initiatives
- Cross-border supervision and exchange of expertise

- Joint monitoring exercises

Greater cooperation would help ensure consistency and strengthen the overall response system of Trusted Flaggers under the DSA.

An important issue raised in discussions is the mental health impact on individuals engaged in monitoring and reporting harmful content. Experience from hotline operators and monitoring organizations shows that staff turnover in these roles can be high due to the psychological burden associated with repeatedly encountering disturbing material.

This raises the question of whether mental health provisions should be integrated into the Trusted Flagger certification process. Organizations conducting monitoring work require sufficient funding to support staff wellbeing, provide training, and ensure that personnel are legally and psychologically prepared to assess content.

Roundtable Session| Collective Advocacy: Opportunities, Gaps and Strategic Directions

Several smaller operational challenges continue to affect the work of Trusted Flaggers:

- Platforms are not always cooperative in practice.
- Reporting channels can be unclear or inconsistent.
- Organizations often have to repeatedly provide the same information to platforms.
- Some platforms rely on geo-blocking rather than removing illegal content from their services.
- Uncertainty remains on how to effectively package systemic risk reports

Democratic spaces, including for Civil Society Organizations, are increasingly shrinking. This raises questions about who should be involved in INACH events and how to strengthen cooperation with other relevant actors, including those that may not serve as Trusted Flaggers. Some participants also noted that economic barriers are making it

difficult for their organizations to continue monitoring online hate speech. Others questioned whether engaging in this work remains worthwhile and, if so, how it can be carried out more effectively.

As online harms increasingly involve AI-generated or manipulated content, Trusted Flaggers require more advanced technical capabilities. This also includes cooperation with Vetted Researchers for the expertise with analytical tools, digital investigation techniques and platform data analysis. . However there is still a lot of uncertainty around the verification process of the Vetted Researcher role.

Trusted Flaggers could also contribute more systematically to regulatory oversight under the DSA by cooperating with Out of Court Settlement Bodies and Vetted Researchers by looking at systemic risks once CSOs send them their reported content.

New initiatives are beginning to support coordination between organizations working in this field. For example, the European Observatory on Online Hate together with INACH have set up an organic coordination structure for organizations interested in becoming Trusted Flaggers or those that have already obtained certification.

Meldestelle Respekt and Debunk.og have been working on two separate inititiatives to set up coordination systems focusing on public reporting, experience sharing and exchange of good practices between Trusted Flaggers.

These operational barriers highlight the need for stronger oversight and clearer procedural guidance. The European Commission is working on Trusted Flagger guidelines and is going to conduct an open consultation on the topic in the coming months.

Recommendations

The panels and roundtable brainstorm session led to a number of recommendations:

- It should be of utmost priority to national DSC's and the EC to ensure the safety and security of Trusted Flagger organisations and other monitoring partners.

- Apart from connecting with national DSC's, it is highly recommended to also establish connections with the representation of the European Commission in the country.
- In order to facilitate cooperation, knowledge exchange on technical issues as well as trends tracking, capacity building and guidance there is a clear need for coordinated efforts for Trusted Flagger organisations.
- There is a need for the guidelines that will be produced by the EC on the Trusted Flagger role to provide a clear structure that includes mental health support for monitoring organisations and their staff together with commitments to protect organisations within the DSA framework in navigating challenges in international- and national political contexts.
- Facilitate cooperation and knowledge exchange between non-Trusted Flaggers and Trusted Flaggers as well, both on a national- and international level. The EC should urge VLOPs to maintain their Trusted Partner programmes and have as many expert organisations as possible during monitoring and reporting.
- In order to ensure the Trusted Flagger organisation can continue to carry out their work on a long term, there is a clear need for funding lines. This has been acknowledged by all institutions and therefore should be a priority for everyone.
- CSOs should consider litigation as part of their strategic toolkit under the DSA. Strategic litigation can help clarify legal obligations, challenge systemic platform practices, and complement regulatory enforcement by creating legal precedents that strengthen accountability.
- The DSA moves the conversation beyond individual pieces of content and focuses on systemic risks on the platforms. Civil society organizations play a crucial role in identifying these risks by documenting patterns of harm, analyzing platform behavior, and providing evidence that regulators can use to enforce the DSA.
- CSOs should consider using Out of Court Dispute Settlements as an avenue to contest the moderation decisions of social media platforms. When provided cases from different contexts and against diverse communities, Out of Court Dispute

Settlement Bodies in cooperation with Civil Society Organisations can support in identifying hate trends, patterns and systemic risks on the platforms.

- Geo-blocking is increasingly used by platforms as a moderation tool under the DSA, but it risks undermining enforcement by allowing content to remain online. Platforms generally argue that they are adhering to the DSA by removing the content where it is illegal. However, illegal content is still harmful for communities (e.g. diaspora) when it is still accessible from a different geographical location. There is a need for DSC's and EU institutions to issue interpretative guidance under the DSA clarifying enforcement expectations. Removal should be the default response for clearly illegal content, while geo-blocking should remain an exceptional measure. To address this, there is a need for stronger transparency reporting, escalation mechanisms for Trusted Flaggers, and cross-border regulatory coordination.
- Expand training initiatives on the international frameworks to address hate speech, the Digital Services Act (DSA), and stakeholder collaboration to strengthen the capacity of organisations working to address online hate speech and foster a coordinated multi-stakeholder approach.