



Bringing the Online In Line with Human Rights



DSA

IMPLEMENTATION REPORT

Compiled by
Adinde Schoorl &
Naomi Tidball
2026

TABLE OF CONTENTS

INTERNATIONAL NETWORK AGAINST CYBER HATE – INACH	2
EXECUTIVE SUMMARY	3
INTRODUCTION	5
CHAPTER 1 MONITORING	7
1.1 MONITORING EXERCISE	7
<i>Removal Rates</i>	<i>8</i>
<i>Feedback Rates.....</i>	<i>9</i>
<i>Response Rates Within 24 Hours</i>	<i>10</i>
1.2. OVERALL PATTERNS AND TRENDS	12
CHAPTER 2. DSA STAKEHOLDERS.....	15
2.1. DIGITAL SERVICES COORDINATORS.....	15
2.2. TRUSTED FLAGGERS	18
2.3. OUT OF COURT DISPUTE SETTLEMENT BODIES.....	23
2.4. EUROPEAN COMMISSION.....	25
CHAPTER 3 TOOLS.....	28
3.1. TRANSPARENCY.....	28
3.2. SYSTEMIC RISKS.....	30
3.3 VETTED RESEARCHERS	32
CONCLUSION & RECOMMENDATIONS	34
RECOMMENDATIONS	35
<i>To the European Commission</i>	<i>35</i>
<i>To Digital Services Coordinators</i>	<i>36</i>
<i>To Online Platforms.....</i>	<i>36</i>
<i>To the DSA Ecosystem.....</i>	<i>37</i>
BIBLIOGRAPHY.....	38

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.

INACH receives funding from various sources, including the European Commission, the SIDN Fonds, and the Dutch Ministry of Interior and Kingdom Relations, along with sponsorships from social media platforms like Google and TikTok, and minor donations from other institutions. The International Network Against Cyber Hate (INACH) unites multiple organizations from Africa, Albania, the EU, Israel, North Macedonia, Russia and South America. 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 Citizenship, 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 Citizenship, Equality, Rights
and Values (CERV) Programme of the European
Union

Executive Summary

The Digital Services Act (DSA) represents the most significant reform of online platform regulation in the European Union to date. By introducing new obligations relating to transparency, illegal content, systemic risks, Trusted Flaggers, Digital Services Coordinators (DSCs), researcher access and platform accountability, the DSA aims to create a safer digital environment while safeguarding fundamental rights. Since its implementation, Trusted Flaggers have been designated across much of the EU, DSCs have become operational, the European Commission has launched multiple enforcement proceedings against Very Large Online Platforms (VLOPs), and new mechanisms for transparency, out-of-court dispute settlement and systemic risk oversight have begun to emerge.

At the same time, this report demonstrates that the practical implementation of the DSA remains uneven and that many of its most innovative mechanisms have yet to reach their full potential. Drawing on the experiences of the INACH network, including the 2025 Monitoring Exercise, a cross-border Holocaust Denial Experiment and practical experiences with Trusted Flaggers and platform reporting, the report identifies persistent shortcomings in platform cooperation, transparency, consistency and accountability.

Although platform responses to notices have generally improved compared to previous years, several recurring challenges remain. Platforms continue to rely extensively on geoblocking and visibility restrictions rather than removing content that appears to violate both national legislation and their own Community Standards.

Reporting systems remain inconsistent across platforms, meaningful explanations for moderation decisions are often lacking, and technical barriers continue to undermine effective notice-and-action procedures. In particular, the inability to report comments through Trusted Flagger channels on certain platforms, such as YouTube, represents a significant enforcement gap.

The publication of the European Commission's draft Trusted Flagger Guidelines is welcomed as an important step towards greater harmonisation. The proposals on standardised reporting channels, APIs, improved onboarding and clearer cooperation between platforms and Trusted Flaggers address many of the practical issues identified during INACH's monitoring activities. However, the report also raises concerns that the Guidelines place extensive obligations on Trusted Flaggers while paying comparatively less attention to platform accountability. Sustainable funding, stronger protection for Trusted Flaggers, clearer performance benchmarks for platforms, and greater transparency surrounding moderation decisions remain necessary to ensure the mechanism can operate effectively in practice.

Overall, the report concludes that the DSA has established a robust regulatory framework, but that its success will ultimately depend on consistent implementation and effective enforcement. Continued investment in civil society participation, stronger cooperation between regulators and platforms, improved transparency, and a greater focus on systemic risks will be essential if the DSA is to fulfil its objective of creating a safer and more accountable online environment.

Introduction

The Digital Services Act (DSA) marks a fundamental shift in the regulation of online platforms within the European Union (EU). By introducing harmonised rules on platform accountability, transparency, systemic risk management, and the handling of illegal content, the DSA seeks to create a safer and more transparent digital environment while safeguarding fundamental rights. Since its entry into application, significant progress has been made in establishing the new regulatory framework. Trusted Flaggers have been designated across the EU, Digital Services Coordinators (DSC) have begun carrying out their supervisory roles, the European Commission (EC) has launched multiple investigations into Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs), and new mechanisms for transparency, researcher access, and independent dispute resolution have started to take shape.

At the same time, the first years of implementation have demonstrated that translating the DSA's ambitious objectives into effective practice remains a complex process. Many of the mechanisms introduced by the Regulation are still evolving, and important questions remain regarding their accessibility, consistency, transparency, and effectiveness. Civil society organisations (CSOs) continue to encounter practical challenges when reporting illegal content, contributing evidence of systemic risks, accessing platform data, engaging with regulators, and monitoring whether platforms are fulfilling their obligations under the DSA.

In 2024, INACH published its first DSA Shadow Report, providing an initial civil society assessment of the implementation of the Regulation and identifying areas where further guidance and enforcement were needed. Two years later, there is now a much clearer picture of how the DSA functions in practice. This second DSA Implementation Report builds on those earlier findings by examining key developments in the implementation of the DSA, highlighting persistent challenges, identifying emerging good practices, and

evaluating the effectiveness of the Regulation from the perspective of organisations working to combat illegal online hate speech and other forms of harmful content.

Drawing on the expertise and practical experiences of the INACH network, this report reviews the functioning of the DSA's core implementation mechanisms, including Trusted Flaggers, DSCs, the EC's enforcement activities, Out-of-Court Dispute Settlement bodies (ODS bodies), transparency reporting, researcher access, and the emerging systemic risk framework. Based on these findings, the report concludes with a series of recommendations aimed at strengthening the implementation, consistency, and effectiveness of the DSA. By identifying both progress and remaining gaps, this report seeks to contribute constructively to the continued development of a regulatory framework that better protects users, upholds fundamental rights, and promotes greater accountability among online platforms.

Chapter 1 Monitoring

Monitoring the implementation of the DSA in practice is essential to understanding whether its new mechanisms effectively address illegal content online. This chapter presents the findings of two monitoring initiatives conducted by INACH and its members: the DSA Monitoring Exercise (ME), which assessed the functioning of platforms' notice-and-action procedures, and a coordinated Holocaust denial reporting experiment examining how major platforms respond to one of the clearest forms of illegal hate speech under the laws of many EU Member States. Together, these exercises provide practical insights into the strengths, shortcomings, and consistency of DSA implementation from the perspective of civil society organisations working on the front line of reporting illegal online content.

1.1 Monitoring Exercise

At the end of 2025, the first Monitoring Exercise (ME) under the revised EU Code of Conduct on Countering Illegal Hate Speech Online+ (CoC+) was carried out. The ME aims to assess how participating online platforms comply with the commitments set out in the CoC+. Over a six-week period, Monitoring Reporters identify instances of illegal hate speech (based on national laws), submit notices to the participating platforms, and monitor the platforms' responses. Following the monitoring period, Monitoring Reporters may discuss individual cases with platforms where necessary, upon initiative by the platforms, before the collected data is submitted to the EC for analysis. The CoC+ has become part of the DSA's co-regulatory framework as a voluntary Code of Conduct under Article 45 of the DSA. While participation remains voluntary, the Code now supports the implementation of the DSA by setting out commitments that contribute to compliance with the Regulation, particularly in relation to the mitigation of systemic risks associated with illegal hate speech. As a result, the Monitoring Exercise has evolved from

assessing compliance with a stand-alone voluntary initiative to evaluating how participating platforms implement their DSA-related commitments. The Code also places greater emphasis on transparency, cooperation with Trusted Flaggers and civil society, improved reporting mechanisms, and the effectiveness of measures to combat illegal hate speech online.

The 2025 Monitoring Exercise introduced several important methodological changes compared to previous editions, which had been conducted annually since 2016. Most notably, reports of illegal hate speech were submitted through the platforms' "illegal under the DSA" reporting channels rather than through standard user reporting mechanisms or Trusted Partner escalation systems. Unlike previous ME's, reported content was therefore no longer escalated through Trusted Partner channels. In addition, cases classified by platforms as "disputed" or "error" cases were excluded from the EC's final dataset. Although discussions took place between Monitoring Reporters and platforms regarding some of these cases, Monitoring Reporters indicated that the exclusion of disputed and error cases from the final dataset occurred without a fully transparent process or clear agreement on how these cases would ultimately be treated. Until 2026, INACH acted as co-organiser of the ME and coordinated the collection and independent analysis of data submitted by numerous Monitoring Reporters. In contrast to the EC's methodology, INACH retained disputed and error cases in its own analysis. As a result, INACH's findings differ from the official figures published by the Commission, particularly in relation to YouTube, where the exclusion of these cases had a significant impact on the reported outcomes.

Removal Rates

INACH

(Data gathered from 22 Monitoring Partners)

- TikTok: 61.6%
- Facebook: 60.4%

- Instagram: 60.8%
- YouTube: 73.1%
- X: 53.2%

EC

(40 Monitoring Partners; disputed and error cases excluded)

- TikTok: 83.8%
- Facebook: 80.8%
- Instagram: 77.9%
- YouTube: 100%
- X: 73.5%

It should be noted that removal rates were generally lower when content was reported through ordinary reporting channels rather than through the “illegal under the DSA” reporting mechanism.

Feedback Rates

The feedback rate refers to the percentage of reports that received a response from the platform, regardless of whether the outcome was a favorable decision or a rejection of the removal request.

INACH

- Facebook: 95%
- Instagram: 86.6%
- TikTok: 81.5%
- X: 59.2%
- YouTube: 19.9%

EC

- Facebook: 99%
- Instagram: 98.2%
- TikTok: 93.8%
- X: 68.5%
- YouTube: 100%

Response Rates Within 24 Hours

INACH

- Instagram: 82.1%
- TikTok: 76.8%
- Facebook: 72.3%
- X: 55%
- YouTube: 19.2%

EC

- Instagram: 67.4%
- TikTok: 88.7%
- Facebook: 87.8%
- X: 64.5%
- YouTube: 97%

(INACH 2025)

(European Commission 2026)

The treatment of reports submitted to YouTube became a particular point of discussion during this ME. YouTube considered an automated notification stating that a report was "under review" to constitute a response to the reporter. Monitoring Reporters, however, argued that such automated acknowledgements should not be regarded as meaningful

feedback. Instead, a response should only be considered complete once the platform has communicated a substantive moderation decision indicating whether the reported content has been removed, retained, or subjected to another enforcement measure.

Another significant finding concerned the increasing reliance on geoblocking rather than the removal of illegal content. In many cases, content reported as illegal under national law remained available on the platform but was merely restricted within the Member State from which the report originated. This suggests that platforms increasingly assess reports within the specific legal context of the reporting country rather than against their own Community Standards. While differences between national hate speech legislation may justify limiting access to content in certain jurisdictions, content that independently violates a platform's Community Standards should generally be removed rather than geographically restricted. The ME nevertheless identified numerous instances in which content that appeared to violate both national law and platform policies was only geoblocked. This raises concerns that geoblocking is increasingly being used as a substitute for effective enforcement. Given the inherently cross-border nature of online communication, including shared languages, cross-border audiences and the widespread use of VPN services, geoblocking offers only limited protection for targeted communities while allowing harmful content to remain accessible elsewhere. Platforms should therefore not rely on geoblocking as a default enforcement mechanism where removal under their own policies is warranted.

The Monitoring Exercise also highlighted a lack of transparency regarding certain moderation measures. On YouTube and X, platforms frequently indicated that content had been "visibility restricted" or otherwise had its distribution limited without explaining what these measures entailed in practice. It often remained unclear whether content was excluded from recommendations, removed from search results, prevented from being shared, or subjected to other forms of reduced distribution. Without clear and standardised explanations of these enforcement measures, monitoring organisations cannot adequately assess whether platform interventions effectively reduced the reach

and impact of illegal content or merely generated a statistical moderation outcome. Greater transparency regarding the practical consequences of all moderation actions is therefore essential.

Despite these concerns, the independently collected data analysed by INACH and several Monitoring Partners indicate an overall improvement in platform performance compared with previous Monitoring Exercises. This assessment is based on the complete dataset, including disputed and error cases. By contrast, the European Commission excluded these categories from its published results, making direct comparisons difficult and, in INACH's view, reducing the reliability and completeness of the published findings. Furthermore, the Commission's report provides limited contextual analysis and does not include visualisations or comparative breakdowns by Member State or platform, reducing its usefulness for identifying trends and informing future improvements to the Monitoring Exercise.

1.2. Overall patterns and trends

One recurring concern was the lack of meaningful feedback provided by platforms. Monitoring organisations frequently received generic responses indicating that it was "unclear what was being reported" or "why the content was considered illegal," without any substantive explanation of the platform's assessment. Such responses provide little insight into how moderation decisions are reached and prevent monitoring organisations from improving the quality of future notices. Greater transparency in platform reasoning is essential to foster effective cooperation between platforms and trusted reporting organisations.

Another significant issue concerns the increasing use of geoblocking rather than the removal of illegal content. Platforms generally maintain that content is geographically restricted only where it violates national law but does not breach their Community

Standards. However, observations from both monitoring exercises suggest that this distinction is not always applied consistently. In numerous cases, content that appeared to violate both national legislation and the platforms' own policies was nevertheless only geoblocked rather than removed. Given the cross-border nature of online communication, geoblocking offers only limited protection to affected communities and should not become a default alternative to meaningful enforcement where removal under platform policies is justified.

Monitoring organisations also continued to encounter longstanding technical and operational barriers that reduce the effectiveness of notice-and-action mechanisms. These included the inability on certain platforms to report comments through Trusted Flagger channels, difficulties obtaining or copying URLs for reported content, and other technical limitations that unnecessarily complicate reporting and documentation. Particularly concerning is YouTube's continued position that comments fall outside the scope of Trusted Flagger reporting mechanisms, despite comment sections being one of the primary locations where hateful and extremist discourse occurs. This creates a significant enforcement gap and is inconsistent with the direction set out in the European Commission's draft Trusted Flagger Guidelines, which recommend that all forms of content, including comments, should be reportable through Trusted Flagger mechanisms.

The monitoring further demonstrated that illegal online hate speech is rarely isolated. Instead, it is embedded within broader and recurring narratives, including anti-immigration rhetoric, Islamophobia, antisemitism, anti-LGBTQ+ "culture war" narratives, and anti-Roma racism. These narratives increasingly overlap and reinforce one another, creating interconnected ecosystems of hate that transcend individual platforms and national borders.

This highlights a broader limitation of the current DSA implementation. Existing notice-and-action mechanisms primarily focus on individual pieces of content, while insufficient

attention is paid to the systemic processes that facilitate and amplify online hate. Coordinated campaigns, algorithmic amplification, bot activity, recommendation systems, and transnational extremist networks all contribute to the spread and persistence of hateful narratives. Addressing individual posts remains essential, but meaningful enforcement under the DSA should increasingly focus on these broader systemic dynamics if the Regulation is to achieve its objective of reducing online harms.

Chapter 2. DSA stakeholders

The effective implementation of the DSA depends on the cooperation of a diverse range of stakeholders, each with distinct responsibilities within the DSA ecosystem. This chapter examines the role and performance of key actors, including Digital Services Coordinators (DSCs), Trusted Flaggers, Out-of-Court Dispute Settlement (ODS) bodies, the EC, researchers and other civil society monitoring organisations. Drawing on implementation experiences and recent developments, the chapter explores how these stakeholders contribute to the enforcement of the DSA, the challenges they face, and opportunities to strengthen cooperation and accountability across the digital governance framework.

2.1. Digital Services Coordinators

To ensure the implementation of the DSA throughout the EU, every EU country has an institution that is responsible for the national process: Digital Services Coordinators (DSC).

As of May 2026, Poland still had not formally designated a DSC. In addition, four other Member States, Czech Republic, Spain, Cyprus, and Portugal, had designated DSCs but had not yet granted them sufficient powers to effectively enforce the legislation (European Commission 2026). As a result, the European Commission referred these five countries to the Court of Justice of the European Union (CJEU) in May 2025 over failures in the implementation of the DSA (Antitrust Intelligence 2025).

In addition, the European Commission sent a formal notice to Croatia regarding insufficient compliance with the implementation of the DSA, specifically concerning the empowerment of the national authority responsible for enforcement (European Commission 2026).

These implementation gaps have also had direct consequences for the rollout of the Trusted Flagger system under the DSA. As of May 2026, several EU Member States still did not have officially designated Trusted Flaggers, including:

- Bulgaria
- Croatia
- Cyprus
- Estonia
- Latvia
- Lithuania
- Malta
- Poland
- Romania
- Slovenia
- Czech Republic

Some countries do have Trusted Flaggers but as organisations often focus on a certain type of illegal content, it means that not all countries have enough Trusted Flaggers that cover all illegal areas.

(European Commission 2026)

The Irish DSC, formally the Irish media regulator Coimisiún na Meán, has become one of the most important regulators under the DSA because many of the world's largest online platforms have their EU headquarters in Ireland. Under the DSA's country-of-establishment principle, the DSC of the Member State where a platform is established becomes the lead regulator for that platform. This means Ireland is the primary DSC for some of VLOPs like Meta, TikTok and YouTube. For ordinary online platforms (non-VLOPs), the lead DSC is often the main enforcement authority. For VLOPs and VLOSEs, the European Commission has direct supervisory powers, but the Irish DSC still plays a crucial role in investigations, information gathering, coordination with the Commission, handling complaints, Trusted Flagger matters, national enforcement issues and participation in the European Board for Digital Services

The Irish regulator is effectively dealing with a disproportionate share of the largest global tech companies operating in Europe. As a result, many CSOs and TF organisations contact the Irish DSC and many DSA complaints end up involving it and therefore it has become a key actor in shaping DSA implementation in the EU. A recurring concern among civil society groups is whether one national regulator can realistically oversee so many major platforms. Criticisms often focus on the resource constraints, the volume of cases, the speed of enforcement and dependence on one Member State for oversight of a large part of the European digital ecosystem (Coimisiún na Meán 2025).

Experiences shared by Trusted Flagger organisations across the EU demonstrate that cooperation with DSCs varies considerably between Member States. While some DSCs have established regular and constructive engagement with civil society organisations, others have had only limited interaction. For example, the Austrian DSC, KommAustria, regularly convenes meetings with national civil society organisations to exchange information on emerging trends, enforcement challenges, and patterns of illegal online content. Similarly, the Irish DSC has actively engaged with civil society through initiatives such as a pilot programme that gathers evidence on systemic issues, rather than focusing solely on individual pieces of content.

These examples illustrate the important role DSCs can play in facilitating cooperation between regulators and civil society. However, such engagement currently depends largely on national practice rather than a coordinated approach under the DSA. While the DSA establishes formal cooperation mechanisms between DSCs through the European Board for Digital Services, no equivalent framework exists for cooperation among Trusted Flaggers or between Trusted Flaggers, other monitoring organisations, and regulators at the European level. Establishing regular national and European forums for dialogue and information exchange would enable Trusted Flaggers to share experiences, identify cross-border trends, discuss implementation challenges, and contribute evidence on emerging systemic risks. Such structured cooperation would strengthen the consistency and effectiveness of DSA enforcement across the EU while making better use of the

expertise developed by civil society organisations through their day-to-day monitoring activities.

2.2. Trusted Flaggers

Trusted Flaggers are independent organisations designated by national Digital Services Coordinators under Article 22 of the Digital Services Act (DSA) because they have demonstrated expertise in identifying and reporting illegal online content. While they do not decide whether content is removed, online platforms are required to give priority to their notices and process them without undue delay. The mechanism aims to improve the detection of illegal content online while ensuring greater transparency, accountability, and cooperation between platforms, civil society organisations, and public authorities. The process of appointing Trusted Flaggers under the DSA is still ongoing. According to the European Commission there are currently over 70 Trusted Flaggers, covering different areas. The number of Trusted Flaggers monitoring content that involves illegal hate speech as a primary or secondary focus is of course a lot lower, around 25 organisations (European Commission 2026).

The experiences of INACH members demonstrate that, while the Trusted Flagger mechanism represents one of the most innovative features of the DSA, important practical and structural challenges remain. These challenges arise both before organisations apply for Trusted Flagger status and after they have been designated.

One of the main barriers to applying for Trusted Flagger status is the absence of structural financial support. The DSA assigns Trusted Flaggers an important role in identifying and reporting illegal content, yet the work requires considerable expertise, staff capacity, legal knowledge, monitoring activities, reporting obligations, and ongoing engagement with platforms and regulators. For many civil society organisations, particularly smaller organisations, these responsibilities cannot easily be absorbed within existing resources. At the same time, organisations that do receive public funding are increasingly accused of acting as instruments of government censorship, creating reputational risks while

receiving little or no remuneration for carrying out a role that is essential to the functioning of the DSA ecosystem. Public attacks against organisations such as Meldestelle RESPEKT in Germany and its director Ahmed Gaafar, accusing him of indirect sympathy for Hamas (Handelsblatt 2024), and the visa ban issued by the US government on Josephine Ballon from the German Trusted Flagger HateAid (The Guardian 2025) illustrate the growing political pressure faced by Trusted Flaggers.

For organisations that have obtained Trusted Flagger status, the application process itself has generally been viewed positively. Several organisations praised the support provided by their DSCs during the designation process. However, experiences with platform onboarding have been far less consistent. While some platforms established efficient contact and training procedures, others lacked designated points of contact, delayed onboarding for weeks or months, or provided no clear information on how Trusted Flaggers could begin submitting notices. In several cases, organisations were unable to use their Trusted Flagger status until the platform itself initiated contact, creating unnecessary delays and administrative burdens.

Although the DSA requires platforms to prioritise notices submitted by Trusted Flaggers, many organisations reported little practical difference between reporting as a Trusted Flagger and reporting through ordinary channels. Delays in processing notices, a lack of confirmation that reports had been received, repeated requests for additional evidence, and limited communication remain common. Smaller platforms often failed to respond to Trusted Flagger notices altogether. Some platforms also continue to lack basic reporting mechanisms. For example, Wikipedia, despite being designated as a Very Large Online Platform, does not currently provide a dedicated reporting mechanism or contact point for Trusted Flaggers. These shortcomings undermine the effectiveness of the mechanism and reduce confidence in the priority treatment envisaged by Article 22 of the DSA.

Several organisations also observed that relationships with platforms have become more formal but less collaborative since the introduction of the DSA. Prior to the Regulation, long-standing monitoring organisations often maintained direct communication channels with platform representatives to discuss complex cases. Today, communication increasingly follows formal procedures, making it more difficult to resolve practical issues or exchange information outside the notice-and-action process.

Trusted Flaggers further identified the absence of structured cooperation between themselves as an important gap in the current DSA framework. While DSCs cooperate through the European Board for Digital Services, no comparable structure exists for Trusted Flaggers or other monitoring organisations. As a result, opportunities to exchange experiences, identify common reporting challenges, share platform responses, or coordinate approaches to emerging trends are largely missed. INACH and the European Observatory on Online Hate (EOOH) have been having regular meetings to fill this void. But a more structured European network would strengthen consistency, facilitate mutual learning, and contribute to a more coherent implementation of the DSA across Member States.

Finally, several organisations questioned the long-term sustainability of their role as Trusted Flaggers. The combination of increasing reporting obligations, annual transparency reporting requirements, limited operational advantages over ordinary reporting, and the absence of financial support has led some organisations to question whether maintaining Trusted Flagger status is feasible. At the same time, organisations also recognised important benefits. In France, for example, Trusted Flagger status has strengthened the position of organisations such as LICRA in their dialogue with the French DSC Arcom, increasing the weight given to their expertise on illegal hate speech. Trusted Flaggers are gradually becoming recognised as one of the key stakeholders, alongside DSCs, the European Commission, researchers, Out of Court Dispute Settlement bodies and platforms, in shaping how the DSA is implemented. That means they are no longer simply reporting illegal content; they are contributing evidence, identifying

enforcement gaps, informing policy discussions and helping regulators understand emerging risks.

The publication of the European Commission's draft Trusted Flagger Guidelines in June 2026 represents an important step towards addressing several of these implementation challenges. The draft provides practical guidance on the designation of Trusted Flaggers, platform obligations, reporting procedures, transparency requirements, and cooperation between stakeholders. It also acknowledges the need for improved onboarding, standardised reporting systems, training, capacity-building, and support for organisations operating in underrepresented fields of expertise. Nevertheless, the draft Guidelines also raise several concerns from a civil society perspective.

In particular, the Guidelines expect Trusted Flagger notices to be highly substantiated, legally reasoned, objective, and consistently accurate. While maintaining reporting quality is essential, this expectation places significant legal responsibilities on organisations that often operate with limited resources. Determining whether content is illegal frequently involves complex legal assessments that ultimately fall within the competence of courts rather than civil society organisations. Good-faith differences in legal interpretation should therefore not automatically be treated as evidence of poor reporting quality.

A further concern relates to the suspension mechanism. Under the draft Guidelines, Trusted Flagger status may be suspended while a DSC investigates whether an organisation continues to satisfy the requirements of Article 22. Although procedural safeguards are provided, organisations may temporarily lose the benefits associated with Trusted Flagger status before any wrongdoing has been established. This may discourage organisations from reporting legally complex or emerging forms of online harm, such as novel hate speech narratives, election-related manipulation, or cross-border legal questions.

Overall, the draft Guidelines place considerable emphasis on ensuring the accountability and reliability of Trusted Flaggers, while comparatively less attention is devoted to ensuring that platforms consistently fulfil their own obligations. Trusted Flaggers are expected to operate as highly professional actors with significant legal responsibilities, yet equivalent guarantees regarding financial support, institutional protection, operational assistance, or effective platform cooperation remain limited. Without addressing this imbalance, there is a risk that the Trusted Flagger ecosystem becomes increasingly cautious, resource-intensive, and less attractive for the diverse range of civil society organisations whose expertise the DSA seeks to harness.

An unintended consequence of the implementation of the DSA has been the changing position of monitoring organisations that do not hold Trusted Flagger status. Many of these organisations have monitored illegal online content for years, developed substantial expertise, and maintained constructive working relationships with online platforms prior to the DSA. Since the introduction of the Trusted Flagger mechanism, however, several organisations have observed that platforms increasingly limit their engagement to formal DSA procedures and are less willing to communicate directly with monitoring organisations that are not designated as Trusted Flaggers. At the same time, these organisations do not benefit from the enhanced recognition and engagement that Trusted Flagger status may provide with Digital Services Coordinators. As a result, valuable expertise and evidence generated by experienced civil society organisations risks being underutilised.

While the Trusted Flagger mechanism is an important component of the DSA, it should complement, not replace, the broader ecosystem of monitoring organisations whose expertise remains essential for identifying emerging harms, supporting victims, and contributing to a comprehensive understanding of online hate and other systemic risks. The draft Trusted Flagger guidelines by the EC also mentions that it encourages platforms to cooperate with other organisations but in practice this happens very rarely.

2.3. Out of Court Dispute Settlement Bodies

Out-of-Court Dispute Settlement (ODS) bodies are independent entities certified under Article 21 of the DSA to provide users with an accessible alternative to challenging content moderation decisions made by online platforms. When a user disagrees with a platform's decision, such as the removal of content, suspension of an account, or refusal to remove reported content, they may submit the dispute to a certified ODS body for review. Users remain free to pursue other remedies, including judicial proceedings. The ODS mechanism was introduced to strengthen user rights, improve accountability in platform moderation, and provide a faster and more affordable alternative to court proceedings. CSOs reportedly are mostly in contact with Appeals Center Europe (European Commission 2026).

The system remains highly fragmented across Member States. Some countries have certified multiple ODS bodies, while others still have none. The European Commission maintains a public overview of certified bodies, but comprehensive comparative evaluations are still lacking (European Commission 2026).

Certified ODS bodies provide users with an independent avenue to challenge content moderation decisions made by online platforms without having to initiate court proceedings. While the DSA requires platforms to engage with ODS bodies "in good faith", it provides little guidance on what this obligation entails in practice. As a result, the extent of platform cooperation is becoming one of the central questions in the implementation of the DSA. This uncertainty is illustrated by the legal challenge brought by X against the certified ODS body Appeals Center Europe (ACE) in Ireland. X disputes ACE's certification and argues that the organisation overstates its authority and role in handling moderation disputes (MLex, 2025). The outcome of this case is likely to clarify the legal obligations of platforms towards ODS bodies and determine whether Article 21 provides an effective system of user redress or merely a symbolic mechanism.

Eighteen months after accepting its first disputes, ACE has published two transparency reports providing the first substantial evidence on how the ODS system functions in practice (Appeals Center Europe, 2026). Between April 2025 and March 2026, ACE received more than 24,000 disputes from users and organisations across the European Union, with the number of eligible disputes increasing ninefold over the reporting period. By March 2026, ACE had issued more than 10,200 decisions, demonstrating both growing awareness of the mechanism and increasing demand for independent review.

The findings reveal significant shortcomings in current platform moderation practices. In cases where ACE was able to review the disputed content, it disagreed with the platforms' decisions in 59% of cases overall. Platform decisions to remove content were overturned in 52% of reviewed cases, while decisions to leave potentially harmful content online were overturned in 63% of cases. Particularly high overturn rates were observed for fraud and scam content (80%), violence and crime (75%), and hate speech (70%). Many of the hate speech cases involved content targeting Roma communities, migrants, religious minorities, women, and LGBTQI+ individuals. These findings suggest that platforms continue to apply their own moderation policies inconsistently, both by removing lawful content and by failing to remove content that violates their Community Standards.

One of the most significant operational challenges identified by ACE concerns platform cooperation. In more than 7,300 eligible disputes, ACE was unable to review the merits of the case because the relevant platform failed to provide the disputed content. As a result, ACE was forced to issue default decisions in favour of users. This problem was particularly acute in account suspension cases and was especially evident in relation to Meta, which reportedly supplied the requested content in fewer than 100 out of more than 4,600 eligible account suspension disputes. Such practices significantly undermine the effectiveness of independent dispute resolution and raise important questions about what the DSA's obligation to cooperate "in good faith" requires in practice.

At the same time, ACE's reports demonstrate the broader value of the ODS mechanism. Beyond resolving individual disputes, its decisions have begun to identify recurring

patterns in platform moderation, including inconsistent enforcement of hate speech policies, repeated failures to remove harmful content, and differences in moderation practices between platforms. In March 2026, ACE shared evidence derived from its cases with the European Board for Digital Services and the European Commission to support discussions on systemic risks under the DSA (Appeals Center Europe 2026).

The experiences of INACH members further illustrate the practical value of the mechanism. DigiQ (Slovakia) and the NEVER AGAIN Association (Poland) submitted several hundred disputes to ACE concerning content targeting Roma communities, migrants, refugees, religious minorities, women, LGBTQI+ individuals, and victims of the Holocaust. In a substantial majority of cases that could be reviewed on their merits, ACE concluded that the platforms had incorrectly left policy-violating content online and overturned their decisions. Both organisations reported very positive experiences working with ACE, highlighting its accessible procedures, professional communication, case-specific guidance, and proactive engagement throughout the dispute process.

Nevertheless, important challenges remain. ODS bodies themselves provide only limited information about their review methodologies, quality assurance processes, and how consistency between reviewers is ensured. Greater transparency regarding assessment criteria and decision-making procedures would strengthen confidence in their work. At the same time, meaningful cooperation from platforms remains essential. Without timely access to disputed content and greater transparency regarding the implementation of ODS decisions, the dispute settlement mechanism cannot fully achieve the objective of providing effective and independent redress under the DSA.

2.4. European Commission

The European Commission plays a central role in the implementation and enforcement of the DSA, particularly in relation to Very Large Online Platforms (VLOPs) and Very Large

Online Search Engines (VLOSEs). The Commission is responsible for supervising compliance with the DSA's obligations on systemic risk assessment and mitigation, transparency, data access, and platform accountability. It has the power to conduct investigations, request information, carry out inspections, impose fines, and adopt enforcement decisions where platforms fail to comply with the Regulation. In addition, the Commission coordinates with national DSCs through the European Board for Digital Services, issues guidance and recommendations on the application of the DSA and plays a key role in ensuring a consistent and effective regulatory framework across the EU.

Since the DSA began applying to VLOPs and VLOSEs, the EC has launched a growing number of investigations and enforcement proceedings against major online platforms. While most cases remain at the stage of formal proceedings, requests for information, or preliminary findings, they provide a clear indication of the Commission's enforcement priorities, including illegal content, child safety, recommender systems, researcher access, transparency, addictive design, election integrity, and broader systemic risks.

X became the first platform to face formal DSA proceedings in December 2023, with investigations focusing on illegal content, notice-and-action mechanisms, disinformation, researcher access, transparency obligations, and algorithmic amplification. In July 2024, the Commission issued preliminary findings that X was in breach of the DSA regarding deceptive interface design, advertising transparency, and researcher access, and in 2026 reportedly expanded the investigation to include recommender systems and so-called "nudification" applications. TikTok has also faced scrutiny, including a preliminary finding in October 2025 that it failed to provide researchers with adequate access to platform data. Meanwhile, Meta's Facebook and Instagram are under investigation for issues relating to child safety, protection of minors, recommender systems, dark patterns, election risks, researcher access, and addictive design. In April 2026, the Commission preliminarily found Meta in breach of DSA obligations concerning underage users, while separate investigations by the Irish Digital Services Coordinator have examined concerns relating to algorithmic manipulation and profiling-based feeds.

Overall, these investigations demonstrate that the Commission is increasingly interpreting the DSA as a broad framework for governing systemic platform risks, moving beyond individual pieces of illegal content to focus on platform architecture, recommender systems, transparency, behavioural design, and the wider societal impacts of digital services (European Commission 2026).

While many investigations remain ongoing and are still at the stage of formal proceedings, requests for information, or preliminary findings, the Commission has now begun issuing final enforcement decisions. In December 2025, the Commission adopted its first DSA non-compliance decision, imposing a €120 million fine on X for breaches relating to deceptive design, advertising transparency, and researcher access (European Commission 2025).

“X will have to pay that fine. The €120 million will have to be paid. We will make sure that we get this money,” Commission Spokesperson Thomas Regnier told reporters during a daily press briefing, when asked how the EU can ensure that X pays the penalty (Politico 2025).

Beyond its enforcement role, the European Commission has increasingly positioned the DSA as a global reference framework for platform governance. Through international dialogues, regulatory cooperation, election integrity initiatives, and exchanges with regulators in jurisdictions such as the United Kingdom, Canada, Australia, Brazil and Japan, the Commission has actively shared experiences from DSA implementation and promoted its approach to platform accountability, systemic risk management, transparency and researcher access. As a result, the DSA is increasingly influencing discussions on digital regulation beyond the European Union (European Parliament 2026).

Chapter 3 Tools

The DSA introduces several important tools to improve platform transparency, accountability, and evidence-based oversight. This chapter examines three key mechanisms: transparency reports, which provide insight into platforms' content moderation practices; the systemic risk framework, which requires VLOPs and VLOSEs to identify and mitigate risks arising from their services; and the vetted researcher regime, which enables independent researchers to access platform data in the public interest. Together, these mechanisms are intended to strengthen scrutiny of online platforms and support a more transparent and accountable digital ecosystem.

3.1. Transparency

Transparency reports are a cornerstone of the DSA, designed to provide regulators, researchers, civil society organisations, and the public with greater insight into how online platforms moderate content and comply with their legal obligations. Under the DSA, online platforms are required to regularly publish information on issues such as content moderation decisions, notices of illegal content, automated enforcement measures, user complaints, Trusted Flagger submissions, and platform resources dedicated to moderation.

Through the DSA Transparency Database, platforms now submit billions of Statements of Reasons for content moderation decisions in near real time, making it possible to analyse moderation practices across platforms and identify broader trends. Early analyses have already highlighted increasing reliance on automated moderation systems, very low user appeal rates, significant differences in enforcement practices between platforms, and disparities across Member States and languages.

A major milestone was reached in early 2026 when VLOPs and VLOSEs published their first fully harmonised transparency reports using the European Commission's

standardised reporting templates. Introduced through the 2024 Implementing Regulation and mandatory from July 2025 onwards, these templates were specifically designed to improve comparability by providing machine-readable and standardised reporting formats. According to the EC, the harmonised templates should enable researchers, regulators, journalists, and civil society organisations to compare platform moderation practices more effectively (European Commission 2024).

Despite these improvements, important shortcomings remain. Transparency reports continue to be highly technical, difficult to navigate, and largely inaccessible to non-specialist audiences. While they provide extensive operational statistics, they often lack the contextual information necessary to meaningfully evaluate platform performance or understand why moderation outcomes differ between platforms.

Research also suggests that harmonisation has not yet resulted in fully comparable reporting. Several studies have found that platforms continue to interpret reporting categories differently, apply automation metrics inconsistently, and submit incomplete or contradictory information (Kaushal et al., 2024). The study 'Disarranged Harmonization of Transparency Reporting by Social Media Platforms Under the Digital Services Act' similarly concludes that important challenges remain despite the introduction of harmonised templates, including inconsistent reporting formats, missing datasets, contradictory reporting methodologies, limited interoperability between reporting mechanisms, and transparency problems that had already been identified in earlier reporting cycles (Cornell University, 2026). Earlier analyses of the DSA Transparency Database reached similar conclusions and identified X as the platform exhibiting the greatest inconsistencies in its reporting practices (Cornell University, 2025).

Beyond data quality, the current transparency framework remains focused primarily on operational indicators, such as the number of notices received, content removals, appeals, complaints, and automated moderation actions. These figures provide valuable insight into the scale of platform moderation but reveal relatively little about its

effectiveness. Transparency reports contain only limited information about broader systemic issues, including algorithmic amplification, recommender systems, coordinated inauthentic behaviour, monetisation incentives, or the systemic dissemination of hate speech and disinformation.

Perhaps the most significant gap is the absence of evaluation metrics. Measures such as precision, recall, prevalence, and error rates are widely used internally by platforms to assess the performance of their moderation systems, yet they are generally not disclosed publicly. These metrics would provide a much more meaningful assessment of whether platforms successfully identify illegal content while respecting users' fundamental rights. Research conducted by the DSA Observatory argues that, despite recommendations made during the legislative process, the DSA ultimately codified largely the same operational metrics that platforms had already been publishing voluntarily, while omitting many of the evaluation metrics needed to independently assess the accuracy and effectiveness of platform moderation systems (DSA Observatory, 2026).

3.2. Systemic risks

A systemic risk exists when the design, algorithms, business model, recommender systems, moderation practices, advertising systems, or platform architecture contribute to broader societal harms. Under Article 34 DSA, systemic risks include actual or foreseeable negative effects arising from the design, functioning, or use of a platform, including dissemination of illegal content, negative effects on fundamental rights, negative effects on democratic processes, civic discourse and elections, public security and public health risks and gender-based violence, protection of minors and well-being. Illegal hate speech primarily falls under Article 34(1)(a): dissemination of illegal content or when it is legal but harmful hate speech it may fall under Article 34(1)(b): negative effects on fundamental rights. Even if some of the content is not illegal under national

law, the platform may still need to assess whether its systems contribute to broader harms.

From a civil society perspective, one of the key challenges surrounding the DSA's systemic risk framework is the absence of clear procedures for external stakeholders to submit evidence of systemic risks to regulators. While NGOs, researchers, and affected communities are often among the first to identify emerging harms, coordinated hate campaigns, algorithmic amplification, or other systemic issues, there is currently no dedicated reporting mechanism, standardised evidentiary framework, or publicly available guidance explaining how such concerns should be documented, submitted, and assessed by the European Commission or Digital Services Coordinators. As a result, organisations frequently face uncertainty about where to direct evidence, what level of proof is required, and how submitted information will be considered within ongoing risk assessments or enforcement proceedings. Greater transparency, clearer channels for engagement, and guidance on evidentiary standards would strengthen the ability of civil society to contribute meaningfully to the identification and mitigation of systemic risks under the DSA.

In practice, most NGOs currently rely on ad hoc meetings with DG CONNECT, consultations, responses to Commission calls for evidence, complaints to DSCs, public reports and media pressure. But none of these constitute a formal systemic risk reporting mechanism. It would be great to create a structured civil society submission process for systemic risks, including guidance on evidentiary standards, submission formats, and feedback mechanisms. That would make the systemic risk framework much more accessible and actionable for NGOs.

3.3 Vetted Researchers

The DSA introduces, for the first time, a legal framework enabling independent researchers to access platform data in the public interest. Under Article 40, vetted researchers may obtain access to data held by VLOPs and VLOSEs for the purpose of investigating and understanding systemic risks within the European Union. Two pathways exist: Article 40(12) facilitates access to publicly available data beyond platforms' voluntary transparency tools, while Article 40(4) allows vetted researchers to request non-public data, such as recommendation metrics, moderation records, and exposure data, through DSCs. These provisions are intended to support research into a broad range of systemic risks, including the dissemination of illegal content, impacts on fundamental rights, democratic processes, public health, and user well-being.

However, the implementation of Article 40 has raised important practical challenges. Researchers may struggle to determine in advance exactly which datasets are necessary to investigate complex platform dynamics, particularly given the DSA's requirement that requested data be both "necessary and proportionate" to a specific research objective. Previous experiences have shown that requests for broader access can be denied on privacy or confidentiality grounds, limiting researchers' ability to explore unknown or emerging risks. Since understanding systemic risks often requires analysing platform-wide behaviour rather than individual user activity, many researchers argue that meaningful oversight depends on access to system-level data that captures how platforms operate as a whole. While challenges relating to platform compliance, technical standards, funding, and data-sharing remain, the DSA nevertheless represents a significant shift in platform governance by establishing a legal basis for independent public-interest research and reducing researchers' dependence on voluntary cooperation from platforms (Arcila et. Al 2026) (Ohme et. Al 2026).

Despite the DSA's groundbreaking provisions on researcher access, significant practical challenges remain. Researchers must demonstrate in advance exactly which data they

require and why access is necessary and proportionate, yet platforms are not obliged to provide a comprehensive overview of the data they hold. As a result, researchers often face an "unknown unknowns" problem, being expected to request data about systems they cannot fully observe.

The process for becoming a vetted researcher is also highly demanding, requiring approval from a Digital Services Coordinator, compliance with strict security requirements, proof of independence, and a clear link between the proposed research and a DSA systemic risk. At the same time, the concept of systemic risk itself remains open to interpretation, creating uncertainty about whether topics such as online hate speech, misogyny, coordinated manipulation, or algorithmic amplification fall within the scope of Article 40. Even where access is granted, platforms may still limit disclosure by citing privacy, confidentiality, trade secret, or security concerns. Finally, existing research APIs often provide only a partial view of platform activity, with important data relating to recommender systems, algorithmic amplification, content visibility, and coordinated networks remaining inaccessible or incomplete. These challenges continue to limit researchers' ability to fully investigate the systemic risks that the DSA seeks to address.

Conclusion & Recommendations

Since the publication of INACH's first DSA Shadow Report in 2024, the implementation of the DSA has entered a new phase. The first two years of practical implementation have demonstrated that the DSA has fundamentally changed the governance of online platforms. Trusted Flaggers have been designated across the EU, DSCs have become operational, the EC has launched multiple investigations into VLOPs and VLOSEs, transparency reporting has become significantly more comprehensive, Out-of-Court Dispute Settlement bodies have started reviewing platform decisions, and the first mechanisms for researcher access and systemic risk oversight have begun to emerge.

These developments represent significant progress. At the same time, the experiences of INACH and its members demonstrate that many of the DSA's most innovative mechanisms have yet to reach their full potential. The Monitoring Exercise, the experiences of Trusted Flaggers, the work of Out-of-Court Dispute Settlement bodies, and the first transparency reports all reveal recurring shortcomings in platform cooperation, consistency, transparency, and accountability.

Perhaps the most important observation is that implementation of the DSA remains largely focused on the moderation of individual pieces of content, while the Regulation itself is built around addressing systemic risks. Illegal content remains the starting point, but the ultimate objective should be to understand and mitigate the systems that facilitate the spread and amplification of illegal hate speech, including recommender systems, algorithmic amplification, coordinated networks, and recurring harmful narratives. Civil society organisations, researchers, Trusted Flaggers, and Out-of-Court Dispute Settlement bodies all generate valuable evidence on these systemic issues. The DSA should make better use of this expertise.

At the same time, the success of the DSA depends on maintaining a strong and diverse civil society ecosystem. Trusted Flaggers perform an essential public-interest function but

continue to face significant operational, financial, and reputational challenges. Experienced monitoring organisations that do not hold Trusted Flagger status risk becoming increasingly marginalised as platforms focus exclusively on formal DSA procedures. The implementation of the DSA should therefore strengthen the entire ecosystem of organisations contributing to safer online spaces, rather than creating a two-tier system of recognised and non-recognised actors. Based on the findings of this Shadow Report, INACH makes the following recommendations.

Recommendations

To the European Commission

1. **Strengthen the implementation of the systemic risk framework** by providing clearer guidance on how evidence from civil society, researchers, Trusted Flaggers and Out-of-Court Dispute Settlement bodies can contribute to systemic risk assessments under the DSA.
2. **Establish sustainable financial and institutional support for Trusted Flaggers**, recognising their essential public-interest role and ensuring that organisations are not discouraged from participating because of financial constraints or reputational risks.
3. **Clarify legal obligations under the DSA**, including platforms' duty to cooperate in good faith with Out-of-Court Dispute Settlement bodies, expectations regarding transparency of moderation decisions, and procedures for reporting systemic risks. Also, clarify the use of geoblocking to avoid a misuse of the option.
4. **Support a permanent European cooperation framework** bringing together DSCs, Trusted Flaggers, monitoring organisations, researchers, ODS bodies, and other civil society organisations to exchange expertise and identify emerging cross-border trends.

To Digital Services Coordinators

5. **Develop structured and regular dialogue with civil society**, including both Trusted Flaggers and other monitoring organisations, through permanent consultation mechanisms rather than ad hoc engagement.
6. **Create clear national procedures for reporting systemic risks**, including guidance on evidentiary standards, reporting formats, and feedback mechanisms.
7. **Invest in capacity building**, training, and the exchange of good practices between Member States to promote consistent implementation of the DSA across the European Union.

To Online Platforms

8. **Improve the transparency and quality of moderation decisions** by providing clear, reasoned, and standardised explanations for content removals, refusals to remove content, visibility restrictions, geoblocking decisions, and appeals.
9. **Standardise and improve reporting mechanisms** across platforms through harmonised interfaces, API-based reporting, comprehensive onboarding for Trusted Flaggers, and reporting functionality covering all forms of content, including comments, live streams, and other platform features.
10. **Strengthen cooperation with civil society** by maintaining constructive engagement not only with Trusted Flaggers but also with experienced monitoring organisations whose expertise continues to provide significant value.
11. **Ensure effective cooperation with ODS bodies** by providing timely access to disputed content, implementing decisions transparently, and informing users about available redress mechanisms.
12. **Move beyond content-by-content moderation** by demonstrating how recommender systems, algorithmic amplification, and other systemic features are being adapted to reduce the spread of illegal hate speech and other societal harms.

To the DSA Ecosystem

13. **Promote cooperation rather than fragmentation** by ensuring that Trusted Flaggers, monitoring organisations, researchers, ODS bodies, and regulators can effectively exchange information, identify emerging trends, and coordinate responses.
14. **Preserve a diverse civil society ecosystem.** Trusted Flagger designation should complement, not replace, the expertise of other monitoring organisations. All qualified civil society organisations should have meaningful opportunities to contribute evidence on illegal content and systemic risks.
15. **Increase transparency and accountability throughout the DSA framework.** Transparency reports, platform reporting systems, Out-of-Court Dispute Settlement decisions, and regulatory processes should increasingly focus not only on operational statistics but also on measuring whether the DSA is effectively reducing systemic risks and protecting fundamental rights in practice.

Bibliography

- Antitrust Intelligence, *'Commission asks Croatia to comply with the Digital Services Act and empower the national authority to enforce it'*, 8 May 2025, [EU Refers Five Countries to Court Over Digital Services Act Failures – Antitrust Intelligence](#)
- Appeals Center Europe, *Transparency Report April 2025 – March 2026*, [Transparency-Report-May-2026-English.pdf](#)
- Botero Arcila, Beatriz; Ramaciotti, Pedro; Cabale, Emma (2026), *'Seeing in the dark: Towards a broad construction of the access to data provisions of the DSA'*, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 15, Iss. 1, pp. 1-24, <https://doi.org/10.14763/2026.1.2085>
- Comisiún na Meán, *'Coimisiún na Meán commences investigations into TikTok and LinkedIn'*, 02 December 2025, [Coimisiún na Meán commences investigations into TikTok and LinkedIn - Coimisiún na Meán](#)
- Cornell University, *'Disarranged Harmonization of Transparency Reporting by Social Media Platforms Under the Digital Services Act'*, Amaury Trujillo, Benedetta Tessa, Stefano Cresci, 17 May 2026, [\[2605.17655\] Disarranged Harmonization of Transparency Reporting by Social Media Platforms Under the Digital Services Act](#)
- Cornell University, *'The DSA Transparency Database: Auditing Self-reported Moderation Actions by Social Media'*, Amaury Trujillo, Tiziano Fagni, Stefano Cresci, 7 February 2025, [\[2312.10269\] The DSA Transparency Database: Auditing Self-reported Moderation Actions by Social Media](#)
- DSA Observatory, *'The Missing Metrics in DSA Content Moderation Transparency'*, 8 January 2026, [The Missing Metrics in DSA Content Moderation Transparency - DSA Observatory](#)

- European Commission, *'Commission asks Croatia to comply with the Digital Services Act and empower the national authority to enforce it'*, 29 April 2026, [Commission asks Croatia to comply with the Digital Services Act and empower the national authority to enforce it | Shaping Europe's digital future](#)
- European Commission, *'Commission fines X €120 million under the Digital Services Act'*, 5 December 2025, [Commission fines X €120 million under the Digital Services Act](#)
- European Commission, *'First results published under the revised Code of Conduct on Countering Illegal Hate Speech Online +'*, 10 April 2026, [First results published under the revised Code of Conduct on Countering Illegal Hate Speech Online + | Shaping Europe's digital future](#)
- European Commission, *'Implementing Regulation laying down templates concerning the transparency reporting obligations of providers of online platforms'*, 4 November 2024, [Implementing Regulation laying down templates concerning the transparency reporting obligations of providers of online platforms | Shaping Europe's digital future](#)
- European Commission, *'Supervision of the designated very large online platforms and search engines under DSA'*, 28 May 2026, [Supervision of the designated very large online platforms and search engines under DSA | Shaping Europe's digital future](#)
- European Commission, *'Trusted Flaggers under the Digital Services Act (DSA)'*, [Trusted flaggers under the Digital Services Act \(DSA\) | Shaping Europe's digital future](#)
- European Parliament, *'EU-UK digital cooperation'*, 15 March 2026, [EU-UK digital cooperation | Epthinktank | European Parliament](#)
- The Guardian, *'European leaders condemn US visa bans as row over 'censorship' escalates'*, 24 December 2025, [European leaders condemn US visa bans as row over 'censorship' escalates | Technology | The Guardian](#)

- Handelsblatt, *'If the new reporting office "Respect!" Censorship?'*, 18 October 2024, [Digital Services Act: If the new reporting office "Respect!" Censorship?](#)
- INACH, 'Monitoring Report 2025', [ME 2026: Monitoring Report, 2025 – INACH](#)
- Kaushal, R, van de Kerkhof, J, Goanta, C, Spanakis, G & Iamnitshi, A 2024, *'Automated Transparency : A Legal and Empirical Analysis of the Digital Services Act Transparency Database'*, in FAcCT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency. Association for Computing Machinery, pp. 1121 - 1132., <https://doi.org/10.1145/3630106.3658960>
- MLex, *"X sues Irish dispute-settlement body, questioning powers and claiming overreach"*, 21 November 2025, [X sues Irish dispute-settlement body, questioning powers and claiming overreach | MLex | Specialist news and analysis on legal risk and regulation](#)
- Jakob Ohme & LK Seiling, *'Finally, Access: How Article 40 DSA Changes Platform Research in Practice'*, 24 April 2026, Political Communication, DOI: 10.1080/10584609.2026.2664157 <https://doi.org/10.1080/10584609.2026.2664157>
- Politico, *'EU says it will 'make sure' Elon Musk's X pays €120M fine'*, 8 December 2025, [EU says it will 'make sure' Elon Musk's X pays €120M fine – POLITICO](#)