w

USER-GUIDE TO THE EU DIGITAL SERVICES ACT

EU DisinfoLab – October 2022

This user-guide will answer all the questions you might have about the Digital Services Act, a groundbreaking law on internet safety and platform accountability.

Latest update: October 2022

Authors: Claire Pershan and Rita Jonusaite, EU DisinfoLab

Disclaimer: The broad political agreement on the Digital Services Act was reached in April 2022 and just voted into law. This document is based on EU DisinfoLab's current understanding of the text. There are still some uncertainties and questions, and EU DisinfoLab will update this document appropriately as our understanding evolves.

EU DisinfoLab
Boulevard Bischoffsheim 39, Boîte 4
1000 Bruxelles
E-mail: info@disinfo.eu

About EU DisinfoLab

EU DisinfoLab is an independent non-profit research organisation specialised in analysing disinformation. We uncover and expose sophisticated disinformation campaigns. We seek to amplify the voices of our community of counter-disinformation experts across the EU and contribute with collective expertise to policy making. You can find more information about our work on our website https://www.disinfo.eu/.

TABLE OF CONTENTS

THE DIGITAL SERVICES ACT 101

What is the Digital Services Act?

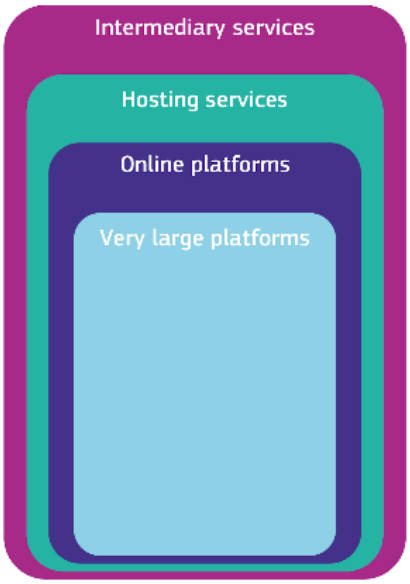
The Digital Services Act (DSA) is a groundbreaking law on internet safety and platform accountability. With this regulation, platforms will be held accountable for their role in disseminating mis and disinformation, among other online harms, and will be required to share more information with researchers and the public.

Ensuring that the EU's Digital Services Act regulation is effective in countering disinformation will take collective effort. That's why EU DisinfoLab has written this "User-Guide to the Digital Services Act". We want you to know what new tools and rights you will have under this law, and we hope that you will get involved strategically.

What digital services does the DSA apply to?

The DSA regulates digital services operating in the EU market or delivering services to EU users.

The regulation sets tiered obligations depending on the type of digital service, with the most impactful obligations applying to "Very Large Online Platforms" (VLOPs) and to "Very Large Online Search Engines" (VLOSEs), with over 45 million users in the European Union. This means that the most impactful elements of the law will relate to platforms like Facebook, YouTube, TikTok, Twitter and services like Google Search[1].



Another category of "Online Platforms" that host user-generated content will also have important responsibilities. This category will include smaller social media platforms, content-sharing platforms, app stores, online marketplaces, and online travel and accommodation platforms. "Hosting Services" refers to cloud service providers (for instance Amazon Web Services, Microsoft Azure, etc.) and to web hosting services that offer infrastructure to support websites. Finally, "Intermediary Services" means services like Internet Service Providers (ISPs) and domain name registrars and registries (like GoDaddy). Mostly we will focus on VLOPs and VLOSEs in this document.

[1] This is our assumption - we are awaiting official designation, or the process through which the European Commission will decide which digital services will qualify as VLOPs and VLOSEs

What is the difference between legal and illegal content, and why does this matter for the DSA?

The DSA differentiates between legal content and content that is illegal according to EU law and the laws of Member States. Disinformation is a bit tricky here, because it often falls into the "grey zone" between what is illegal and legal. Some elements of disinformation campaigns may be illegal in some member states, for instance harassment or defamation. However, generally disinformation is understood to be harmful but *legal*, like spreading conspiracy theories.

The DSA sets obligations for how digital services deal with illegal content. We will not go over those provisions in detail here since we are focused on disinformation. But the DSA does set obligations for how digital services deal with content that has societal risks, and disinformation clearly fits here. The DSA also has obligations for how platforms deal with violations of their terms of service, and disinformation fits here as well. Because disinformation is harmful to users, social media platforms have generally approached the problem through their terms of service or community guidelines.

KNOW YOUR RIGHTS UNDER THE DSA

What can I do if I want to report disinformation? Does DSA make a difference there?

DSA **does not establish** a new or obligatory reporting system specifically for disinformation, only for illegal content. However most online platforms already have tools in place which you can use to report content that is incompatible with platform terms and conditions, which is often the case for disinformation.

What can I do if I reported disinformation and nothing happened?

You can use the *Internal complaint handling system* provided for in the DSA (Article 20). All online platforms will need to have a system allowing users to complain about platforms' content moderation decisions, both in cases of over-moderation (take downs) and under-moderation (when platforms decide not to act on reported content or when the content moderation decision was not adequate). Platforms will need to either adapt existing mechanisms, or create new ones, that allow these complaints.

Importantly, when your complaint contains sufficient grounds that the platform considers it was wrong not to act, or that it was wrong to act, it would need to reverse its decision as quickly as possible or inform you about the other redress possibilities.

Information regarding rules of procedure of the functioning of internal complaint handling systems should be provided in a platform's terms and conditions.

How is it useful for me? For those fighting disinformation and often receiving no reaction from platforms when disinformation is identified and reported to them, **Article 20 of the DSA** makes sure that the decision not to act is seen as a content moderation decision and can be challenged. This has been one of the key things that the EU DisinfoLab advocated for in the DSA, and we are happy to say this is a win for us and for the entire counter-disinformation community.

Who will have to comply? All online platforms except micro and small ones.

- A microenterprise employs fewer than ten persons and its annual turnover and/or annual balance sheet total does not exceed €2 million.
- A small enterprise employs fewer than 50 persons and its annual turnover and/or annual balance sheet total does not exceed €10 million.

Does this mean small and micro enterprises are exempt from the regulation?

No, small and micro enterprises still have obligations, for instance related to tackling illegal content (more on this below when we discuss Article 16). If they wish they can also join any voluntary Codes of Conduct, for instance related to tackling disinformation.

What if I am not satisfied with the outcome of my complaint? Is there anything I can do to challenge this decision?

Yes, you can. If you reported a piece of disinformation, it was not acted upon or you believe not adequately moderated, and the outcome of the complaint under article 20 is not satisfactory, you can challenge the platform's decision on this through yet another tool: *Out-of-court dispute settlement,* provided for in the DSA (Article 21). The article allows the establishment of independent bodies in different Member States through which you could settle disputes without going to an official court. These bodies would be certified by the Digital Service Coordinators (DSC) of the Member States.

While these out-of-court dispute settlement bodies will not be able to impose a binding solution, the DSA requires both parties, meaning the user and the platform, to take part in the dispute settlement process. If the out-of-court dispute settlement body decides in favour of the user, the platform would need to cover all procedural costs. If the decision is in favour of the platform, the user would not have to cover any costs incurred by the platform. In other words, you as the user would only be charged if it was found that you brought the dispute in bad faith. The accessibility of the out-of-court dispute settlement for users is ensured by mandating this service either free of charge or only taking a nominal fee from the user.

How is it useful for me? Since disinformation is not generally illegal content and usually not defined in national laws, you usually cannot bring your problem to a national court. Out-of-court dispute settlement is the best option to challenge the platform's decision in case you are not satisfied with the outcome of the initial internal complaint procedure (Article 20). It gives you additional tools to appeal and seek redress.

Who will have to comply? All online platforms except micro and small ones.

Is there anyone else who can help me to defend my rights under DSA? Can I help someone to defend theirs?

Yes, there is a *Representation* provision in the DSA (Article 86) that gives you a right to mandate a body, organisation, or association to exercise your rights provided in the DSA on your behalf (for example under Article 20 & 21). Also, complaints submitted on behalf of the users through mechanisms referred to in Article 20 are processed and decided upon with priority.
Organisations wanting to take up this role should be non-profit, established in a Member State, and its statutes to demonstrate legitimate interest in ensuring that the DSA is complied with.

How is it useful for me? This would allow you to either ask a specialised organisation to seek redress on your behalf. This also potentially lets you become a specialised organisation representing victims of disinformation. The priority given to complaints submitted by representative organisations would also mean that urgent matters, such as no action on a far-reaching disinformation campaign, would be dealt with more quickly.
Who will have to comply? All online platforms except micro and small ones.

Okay… so this is all about what I can do when I spot disinformation online. What can I do to help prevent disinformation or reduce its spread in the first place?

VLOPs and VLOSEs will need to conduct *risk assessments* and design appropriate *risk mitigation measures* under the DSA (articles 34 and 35) to provide safer services for users, including assessing and mitigating risks for disinformation. VLOPs and VLOSEs where appropriate, will need to consult, among others, independent experts, and civil society organisations.

Systemic risk assessment will need to look at how their services contribute to the spread of disinformation, including through algorithmic systems, content moderation systems, applicable terms and conditions, advertisement, and data collection practices. Particular attention should be given to inauthentic use of their systems. It also sets a requirement for users to label “deepfakes” by obliging platforms to give users a tool to indicate that their content is synthetically manipulated to deceive. If platforms fail to comply with this or any other obligation under the DSA, they will face fines up to 6 percent of their annual worldwide turnover, and 1 percent if they provide incorrect or misleading information.

How is it useful for me? The requirement for platforms to consult civil society organisations when identifying their systemic risks and then to put forward risk mitigation measures gives us in the counter-disinformation community the grounds to request a seat at the table in the process through which VLOPS and VLOSEs, and the Commission enforce the DSA. While collaborating with civil society is not a direct legal obligation, the DSA can incentivise platforms to engage with you.

Who will have to comply? VLOPS and VLOSEs.

Can I submit a complaint about a platform?

You have the right to submit a complaint to your Digital Services Coordinator (DSC) about any platform you are using if you want to allege that they have infringed the regulation or if you want to seek damages (Article 53). This can also be done by an organisation or association on your behalf if that organisation has legal rights as a representative organisation under the DSA (Article 86). Your DSC will assess your complaint and submit it to the DSC of the member that is overseeing the regulation of the platform.

What is the relationship between the DSA and the new Code of Practice on Disinformation?

The Code of Practice has been strengthened with more precise commitments for the signatories and will link up with the DSA. It will become a Code of Conduct under Article 45 of the DSA. However, it remains voluntary. Signatories can join the Code as a way to show they are mitigating their systemic risks related to mis/disinformation. They can become a signatory to the entire Code and then adhere to certain commitments based on their systemic risks.

The updated Code of Practice on Disinformation has been revealed. Details about the exact relationship between the Code of Practice and the DSA remain to be worked out, however, according to the European Commission, non-compliance by VLOPs and VLOSEs who sign up to the Code as a system risk mitigation measure would lead to fines. Other details also need to be figured out, such as the processes for auditing, etc.

What about the illegal content? What are some of the mechanisms in place to report that? Are they different from the ones that I can use to report disinformation?

DSA mandates platforms to create *notice and action mechanisms* that users can employ to report illegal content (Article 16). After the submission of a notice, the service provider should get back to the user without delay about the service provider's decision on the reported content and redress possibilities.

How is it useful for me? You can use the notice and action mechanism to report illegal content and be sure that service providers will need to inform you about their decision on it.

Who will have to comply? All hosting services.

Can I know why the service provider decided to take a certain action on my content?

Yes, in the DSA according to the *Statement of reasons* (Article 17) hosting services will have to provide reasons to any affected recipient of the service on any restrictions on visibility of the content, restrictions of monetisation of the content, suspension, or termination of the service in whole or in part, also of recipient's accounts. This statement would need to explain what action has been taken and the grounds on which it is either illegal or incompatible with the platform's terms and conditions.

The statement must also share clear and user-friendly information on redress mechanisms available.
An important safeguard here has been added where the statement of reasons would not apply in case of intentional manipulation of the service, for example in case of those running coordinated disinformation campaigns. These bad actors should not be able to obtain knowledge that would help them circumvent the platforms' policies.

How is it useful for me? This will bring much more transparency about the decisions that platforms take in their content moderation efforts and help you understand their arguments in case you would like to appeal or challenge their decisions.

Who will have to comply? All hosting services.

How does DSA affect my status as a Trusted Flagger?

Trusted Flaggers: Article 22
There will be a formal regime of DSA Trusted Flaggers specifically under DSA: this is a status that will be granted to an entity upon its application to the Digitals Services Coordinator in their Member State. Notices submitted by these Trusted Flaggers on illegal content are treated with priority.
It is not clear from the text what kinds of illegal content areas these DSA Trusted Flaggers will work on, but because the text refers to illegal content in Article 22, it seems they will be focused on illegal content.

However, if you already hold the status of a Trusted Flagger with respect to certain platforms, for instance Trusted Flagger for disinformation, the DSA will likely not change this, and this status should still be respected.

In order to be granted the status of DSA Trusted Flaggers, you as an entity must meet predefined criteria such as a specific expertise in illegal content, independence from the platforms and integrity of its activities. The DSA Trusted Flaggers should publish reports at least once a year on their activities.

How is it useful for me? Notices submitted by Trusted Flaggers will have priority review, so this ensures that the reported content is removed more quickly.
Who will have to comply? All online platforms except micro and small ones.

What does the DSA say about ads?

Platforms will no longer be allowed to target ads based on behavior for minors or based on profiling sensitive categories of personal data for anyone (like ethnicity, political views, or sexual orientation). They will have to inform users when they are targeted by an ad, who paid for the ad, when content is sponsored, and when influencers are promoting commercial messages.

Platforms must create ad repositories, allowing researchers, civil society groups and regulators to inspect ad placement and targeting. And they must assess if their advertising systems are manipulated or otherwise contribute to societal risks, for instance the risk of promoting or funding disinformation.

What happened with the “media exemption” in the DSA?

There were attempts to introduce the media exemption excluding media content from content moderation. This would have provided default legal protection to all content published by a “media”, shielding them against any content moderation efforts by platforms.

Media had a very vague definition and is generally impossible to define, so this would have potentially shielded many actors from content moderation and opened the floodgates to disinformation.

These attempts have been rejected by the European Parliament and the Council of the EU thanks to the work of the disinformation and digital rights community. Hence, we have no “media exemption” in the DSA.

What new data will be available?

The DSA will create important new data sets. Disinformation experts will be able to use the new data created from transparency obligations to ensure that platforms are complying with the regulation and to “look under the hood” and better understand the challenges that exist.

- **Article 15:**

All intermediary services will have to publish detailed yearly reports about their content moderation, including:

- the number of notices submitted through the notice and action procedure
    - the number of removal orders received from Member States’ authorities, categorised by type of illegal content
    - the number of notices submitted by trusted flaggers
    - any action taken on the notices and whether it was because the content was illegal or because it violated terms and conditions
    - the number of notices processed exclusively by automated means
    - the median time needed for taking the action
- the use of automated tools

- the measures taken to provide training and assistance to persons in charge of content moderation
- **the complaints received through the internal complaint-handling system**
    - the basis for those complaints
    - the decisions taken
    - the median time needed
    - the number of instances where those decisions were reversed

- **Article 24:**

Additional reporting obligations apply to online platforms and to VLOPs.

A Commission Database will contain the decisions and the statements of reasons related to removing illegal content.

Every six months online platforms must publish data on their average monthly users in each Member State.

In their yearly transparency reports (above) they must also include:

- the number of disputes referred to the out-of-court dispute settlement bodies, their outcomes, and the average length of those procedures
- the number of suspensions and reason for suspensions related to
- any use made of automatic means for content moderation and data about accuracy

- **Article 26:**

Platforms must provide users with specific information on their advertisements in real time, including:

- that the information displayed amounts to an advertisement
- the natural or legal person on whose behalf the advertisement is displayed
- information about the main targeting parameters

- **Article 39:**

Ad transparency obligations for the VLOPs require them to set up a public online interface that can be used to search for:

- the content of the advertisement
- the natural or legal person on whose behalf the advertisement is displayed
- the period during which the advertisement was displayed
- whether one or more particular groups of users were the intended target
- the main targeting parameters
- the total number of users reached
- aggregate numbers for the group or groups of users to whom the advertisement was targeted specifically

- **Article 40:**

The DSA will set up a framework to force VLOPs to provide access to data to vetted researchers. Vetted researchers may include civil society organisations that meet specific criteria. Details here remain to be determined. The researcher requests will have to go through the national-level regulator (the “Digital Service Coordinator”). These requests must be for the purpose of monitoring the VLOPs systemic risks and compliance with the requirement to mitigate these risks. For example, a researcher could submit a request for data related to assessing the effectiveness of their counter-disinformation efforts.

The DSA also provides some examples of types of data that will be available in Recital 98, for instance, where technically possible, real-time data on "aggregated interactions with content from public pages, public groups, or public figures, including impression and engagement data such as the number of reactions, shares, comments from recipients of the service."

- **Article 42:**

VLOPs must also publish yearly a report outlining the outcome of the systemic risks assessment, the risk mitigation measures, the audit report, and the audit implementation report.

Who is responsible for enforcing the DSA?

The DSA has a two-tiered enforcement structure. The VLOPs and VLOSEs will be overseen by the European Commission. This is intended to ensure strong enforcement of the largest platforms even if there is not sufficient political will or resources in each Member State.

Then, all other services will be overseen by the nationally appointed regulators. Each Member State will create a Digital Service Coordinator (DSC) who will be the main entity responsible for overseeing the regulation in the country. Member States can appoint multiple regulators to oversee different aspects of the regulation, but they need one DSC.

What are the powers of the Digital Service Coordinators?

The DSC will have many important powers. For instance, they will be responsible for approving data access requests (under Article 40), designating Trusted Flaggers (under Article 22), designating out of court dispute settlement bodies (under Article 21), and receiving complaints (Article 53). The DSC also has the ability to request relevant (compliance-related) information from the digital services it oversees and to conduct on-site inspections.

DSCs are also encouraged to develop national tools and guidance for digital services. For instance, they are supposed to give guidance to platforms about setting up the complaints' mechanisms discussed earlier.

What is the European Board for Digital Services?

Representatives of the Digital Service Coordinators will together make up the European Board for Digital Services, an EU level independent advisory group that will oversee the proper application of the regulation.

The Board may invite experts and observers to its meetings (Article 62) and may cooperate with external experts. They must disclose these consultations. It is therefore possible for us as civil society and disinformation experts to advise the Board and sit in on meetings – this could be an important way for us to get insights into the functioning of the regulation.

Who will be my DSC?

The DSCs will be designated by the national governments. If they wish, Member States can designate an existing national authority as their DSC. DSCs must have sufficient resources and must have complete independence from private and public bodies.

Governments should be thinking now about who their DSC will be, since the DSC should be ready to enforce the regulation in 15 months from now.

What if my DSC isn't doing their job properly?

If you are having problems with the Digital Services Coordinator in your Member State, you may be able to seek help from a different Digital Services Coordinator. For each digital service under the regulation, there is a DSC of Establishment (in the member state where they are legally registered), and the various DSCs of Destination (where they operate).

A DSC of Destination can request the DSC of Establishment to take investigative or enforcement actions towards the platform in its jurisdiction. Also, in cases involving at least three Member States, the Board can request the DSC of Establishment to take these actions.

Keep in mind that the European Commission still has the role of overseeing VLOPs and VLOSEs.

What if my Trusted Flagger request is denied?

Civil society fought hard to try to ensure an 'appeals' process for cases when these requests were denied by your DSC but unfortunately did not win this.

What if my research or data access request is denied?

There is currently no appeals process if your data access request is denied by your Digital Services Coordinator. However, the European Commission will establish an independent agency to advise on the request vetting process.

The Delegated Act that will detail Article 40 on Data Access & Scrutiny might provide further provisions on data access requests.

Who can I contact at each platform regarding the regulation?

All digital services in scope of the regulation must have a single point of contact (Article 11). The single point of contact is necessary for communicating with the national government authorities (like the DSC), the European Commission, the European Board for Digital Services, and recipients of the service (you!). The single point of contact is required to be easily contactable and responsive to your requests.

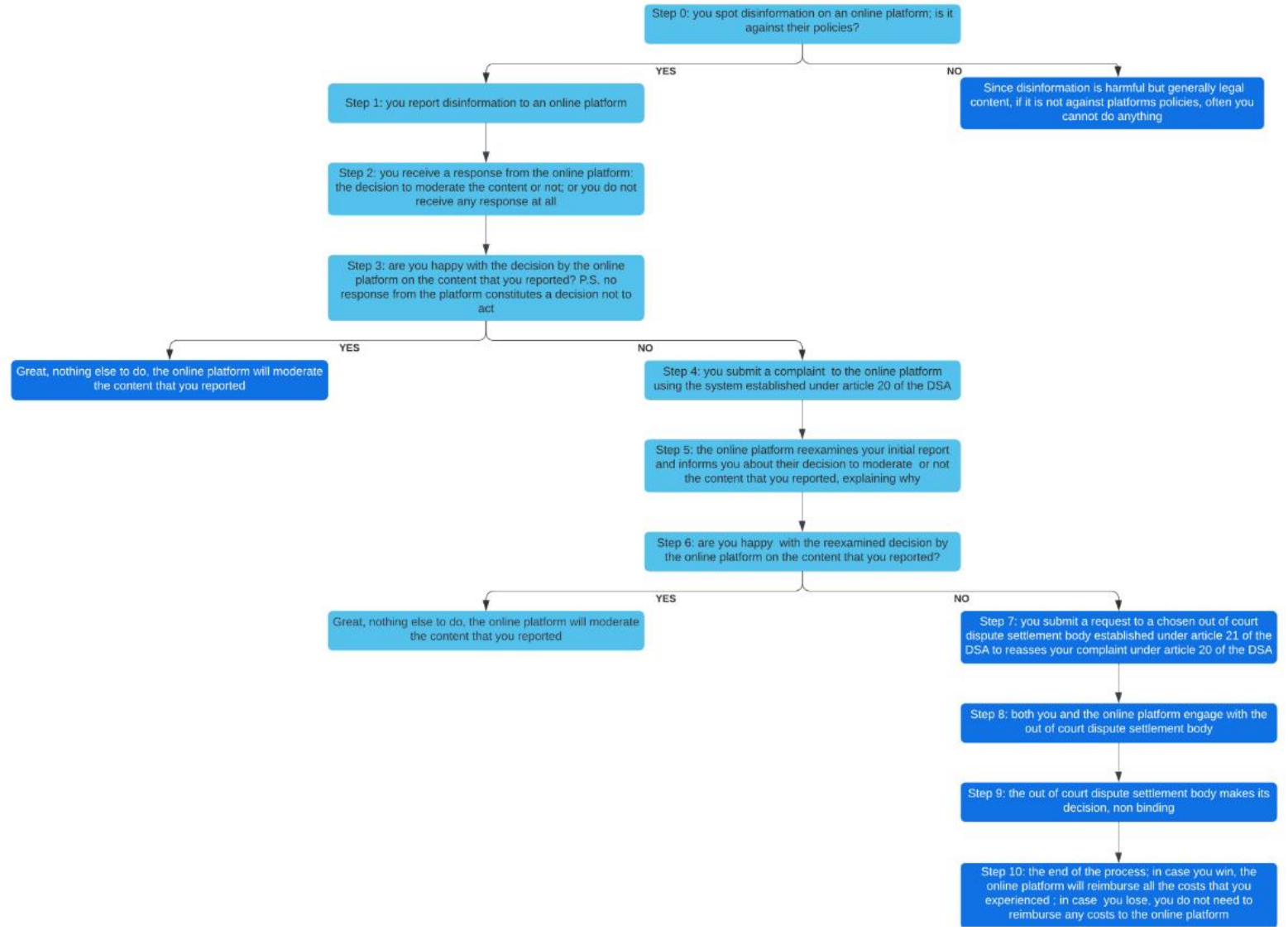
Digital services that are not legally established in the EU must appoint a legal representative (Article 13) in an EU country where they offer services. This representative is responsible for cooperating with the member state's authorities, the Commission, and the Board, and can be held liable for non-compliance with the Regulation.

What are the next steps for enforcing the regulation?

Because it is a regulation, it will apply directly to all countries in the EU. It will apply fifteen months after "entry into force" or from January 1, 2024, whichever later.

However, the regulation will apply to VLOPs and VLOSEs at an earlier date, four months after these services are designated as VLOPs and VLOSEs.

DSA REPORTING PROCESS OVERVIEW



FURTHER RESOURCES

The European Commission has an official Questions and Answers page:
https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers

Julian Jaursch, working at the Stiftung Neue Verantwortung (SNV), has an overview of the Digital Service Coordinator's role and enforcement generally:
https://www.stiftung-nv.de/de/publication/dsa-why-germany-needs-strong-platform-oversight-structures

The Center for Democracy and Technology has an overview of the transparency obligations in the DSA:
https://cdt.org/wp-content/uploads/2021/06/2021-06-18-CDTEU-Overview-of-transparency-obligations-for-digital-services.pdf