Digital Services Act

What is the Digital Services Act (DSA)?

The Digital Services Act (DSA) is a new set of EU-wide rules for digital services acting as intermediaries for consumers and goods, services, and content. In the context of the DSA, digital services refer to intermediary services such as host providers, online marketplaces, and social media networks.

The DSA aims to build a safer and fairer online world. It will introduce rules that equally protect all users in the EU, both in regard to illegal goods, content or services, and their fundamental rights.

For example, it ensures:

- an easy way to report illegal content, goods, or services;
- stronger protections for people targeted by online harassment and bullying;
- transparency around advertising;
- bans on certain types of targeted advertising, such as those using sensitive data or the data of minors;
- easy-to-use, free-of-charge complaint mechanisms for if an online platform takes our content down;
- simplified terms and conditions.


Where can I read the Digital Services Act?

The Digital Services Act (DSA) is published on the EUR-Lex website. You can read it in any official EU language.


Will the Digital Services Act (DSA) replace the e-Commerce Directive?

The Digital Services Act (DSA) does not replace the e-Commerce Directive.

However, in order to achieve greater harmonisation, the DSA incorporates the existing liability exemption rules of the e-Commerce Directive which ensure that intermediary services can continue to thrive in the single market.

How does the Digital Services Act interact with the General Data Protection Reguation (GDPR)

The Digital Services Act (DSA) aims to complement the rules of the GDPR to ensure the highest level of data protection.

For example, in regard to the processing of personal data for advertising purposes, providers of platform services are simultaneously in scope of the DSA and the GDPR.

In addition to the GDPR-conditions for any personal data processing, the DSA prohibits that providers of online platforms target advertisements using user profiling that relies on the special categories of data specified in Article 9(1) of the GDPR, such as sexual orientation, ethnicity or religious beliefs.

Moreover, any use of profiling to present targeted advertisements is prohibited, when the providers are aware with reasonable certainty that the user is a minor.
Why is it necessary to regulate digital services on a European level?

Due to uncoordinated regulatory efforts at national level, the regulatory issues covered under the Digital Services Act are subject to multiple divergent rules in different Member States, causing confusion among businesses and citizens alike. The DSA aims at streamlining the laws, by defining a single set of EU-wide rules and establishing a coordination and enforcement networks across all Member States.

What is the difference between Digital Services Act and Digital Markets Act?

The Digital Services Act (DSA) covers online intermediaries and platforms (for example, online marketplaces, social networks, content sharing platforms, app stores, and online travel and accommodation platforms) with the aim to set out a new standard for the accountability of online platforms regarding disinformation, illegal content, and other societal risks. It includes overarching principles and robust guarantees for freedom of expression and other fundamental rights.

The Digital Markets Act (DMA) includes rules that govern gatekeeper online platforms. It aims to ensure that such platforms behave in a fair way online. These rules will help to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally.


Who does the Digital Services Act apply to?

The Digital Services Act (DSA) applies to all online intermediaries and platforms in the EU, for example, online marketplaces, social networks, content sharing platforms, app stores, and online travel and accommodation platforms.

Small and micro-enterprises are exempted from some rules that might be more burdensome for them. The Commission will carefully monitor the effects of the new Regulation on SMEs.

Very large online platforms and search engines (VLOPs and VLOSEs) have additional obligations.

What are very large online platforms and very large search engines?

Very large online platforms and search engines are those whose average users reach or exceed 10% of the EU population. This is equivalent to having 45 million users or more.

See below for the list of designated VLOPs and VLOSEs the Commission has designated so far.

VLOPs:

- Alibaba AliExpress
- Amazon Store
- Apple AppStore
- Booking.com
- Facebook
- Google Maps
- Google Play
- Google Shopping
- Instagram
- LinkedIn
- Pinterest
- Pornhub
- Snapchat
- Stripchat
- TikTok
- Wikipedia
- X (formerly known as Twitter)
- Xvideos
What does the designation as VLOP or VLOSE mean for online platforms?

Very large online platforms (VLOPs) and search engines (VLOSEs) need to meet a number of obligations such as:

- carrying out risk assessments;
- introducing risk mitigation measures;
- providing easy to read and multilingual versions of their terms and conditions;
- putting in place a crisis response mechanism;
- creating a public repository for the advertisements used on their services.

Moreover, they are required to implement these obligations 4 months after their designation. This means that for VLOPs and VLOSEs designated in April 2023, these obligations already apply.

What is the timeline of the Digital Services Act?

The Digital Services Act (DSA) was proposed in December 2020. Political agreement was reached in April 2022, and it entered into force in November 2022.

By 17 February 2023, platforms and search engines were obliged to publish their user numbers. The Commission designated the first very large online platforms and search engines (VLOPs and VLOSEs) on 25 April 2023 and the second batch on 20 December.

Platforms designated as VLOPs or VLOSEs have 4 months from designation to comply with DSA rules, which includes the publication of a risk assessment.

All regulated entities will need to comply with the DSA by 17 February 2024. This is also the deadline for Member States to establish Digital Services Coordinators.

Users

How will the Digital Services Act protect my fundamental rights?

The Digital Services Act (DSA) introduces a number of rules to protect our fundamental rights online. These rights include freedom of thought, freedom of expression, freedom of information and freedom of opinion without manipulation.

The DSA ensures:

- transparency of content removal decisions and orders;
- publicly available reports on how automated content moderation is used and its error rate;
- harmonisation of responses to illegal content online;
- less dark patterns online;
- a ban on targeted advertising using sensitive data or the data of minors;
- greater user transparency on their flow of information, such as information on parameters of recommender systems and accessible terms and conditions.

Users

How will the Digital Services Act protect my fundamental rights?

The Digital Services Act (DSA) introduces a number of rules to protect our fundamental rights online. These rights include freedom of thought, freedom of expression, freedom of information and freedom of opinion without manipulation.

The DSA ensures:

- transparency of content removal decisions and orders;
- publicly available reports on how automated content moderation is used and its error rate;
- harmonisation of responses to illegal content online;
- less dark patterns online;
- a ban on targeted advertising using sensitive data or the data of minors;
- greater user transparency on their flow of information, such as information on parameters of recommender systems and accessible terms and conditions.

Read more about what the EU is doing to protect our rights online (https://digital-strategy.ec.europa.eu/en/policies/digital-principles)
What are dark patterns?

Dark patterns are a way of designing online platforms to trick users into doing things they otherwise would not have considered, often but not always involving money.

For example, platforms might trick users into sharing more information than they would otherwise agree to. Or, they might advertise a cheaper but unavailable product and then direct the user to similar products that cost more. Other examples include tricking users to subscribe to services, hiding or creating misleading buttons, making it difficult to unsubscribe to newsletters and more.

The Digital Services Act (DSA) contains an obligation that equates to a ban on using so-called dark patterns on online platforms. Under this obligation, online platforms will have to design their services in a way that does not deceive, manipulate or otherwise materially distort or impair the ability of users to make free and informed decisions.

How will the Digital Services Act help tackle disinformation?

The Digital Services Act (DSA) introduces a number of obligations to tackle the spread of disinformation.

Firstly, it requires VLOPs and VLOSEs to perform risk assessments on various elements of their services. The risk assessments should include risks stemming from their design, functioning or use such as coordinated disinformation campaigns. The assessment should consider how the services of the VLOP or VLOSE are used to disseminate or amplify misleading content. Based on the risk assessments, online platforms are obliged to implement risk mitigation measures.

Secondly, VLOPs and VLOSEs need to have a crisis response mechanism. This should include measures to take when their platform is used for the rapid spread of disinformation.

Thirdly, the DSA encourages platforms to sign up to the voluntary code of practice on disinformation.

Finally, the DSA recognises the role that targeted advertising can play in spreading disinformation. As well as rules limiting targeted advertising, the DSA requires VLOPs and VLOSEs to maintain a public advertisement repository. These repositories will help researchers study emerging risks, such as disinformation campaigns which negatively affect public health, security, civil discourse, political participation, or equality.

Read more about what the Commission is doing to tackle disinformation.

How does the DSA tackle illegal content online?

The DSA requires platforms to have easy-to-use flagging mechanisms for illegal content. Platforms should process reports of illegal content in a timely manner, providing information to both the user who flag the illegal content and user who published the content on their decision and any further action.

Does the Digital Services Act define what is illegal online?

No. The new rules set out an EU-wide framework to detect, flag and remove illegal content, as well as new risk assessment obligations for very large online platforms and search engines to identify how illegal content spreads on their service.

What constitutes illegal content is defined in other laws either at EU level or at national level - for example terrorist content, child sexual abuse material, or illegal hate speech is defined at EU level. Where a content is illegal only in a given Member State, as a general rule it should only be removed in the territory where it is illegal.

What is changing in regard to content moderation?

The DSA obliges platforms to have a point of contact for users, such as email addresses, instant messages, or chatbots. Online platforms will also have to ensure that contact is quick and direct and cannot solely rely on automated tools, making it easier for users to reach platforms if they wish to make a complaint. Secondly, online platforms must ensure that complaints are handled by qualified staff, and that the matter is handled in a timely, non-discriminatory manner. Online
platforms must also provide clear and specific reasons for their moderation decisions. Thirdly, if a user chooses to have a decision reviewed, this must be handled free of charge via a platform’s internal complaints system.

At present, the only way to settle a dispute between user and platform is through the court. Starting from 17 February 2024, after the full application of the DSA, users will be entitled to an out of court dispute settlement. The cost of this should be affordable and borne by the platform they use.

**What is a statement of reasons?**

If online platforms decide to remove a piece of content, they now need to provide to any affected user information called “statement of reasons”, detailing why that content was removed or limited.

VLOPs must also send these statements of reasons without any personal data to a collective database, called the DSA Transparency Database ([https://transparency.dsa.ec.europa.eu/](https://transparency.dsa.ec.europa.eu/)). The DSA Transparency Database allows researchers to consult an unprecedented amount of content moderation decisions and study the evolution of the systemic risks covered by the DSA.

**Does the Digital Services Act limit targeted advertising?**

The Digital Services Act (DSA) makes advertising more transparent, ensuring that it is clearly labelled, and that information is available about who is placing the ad and why you are seeing it.

It also introduces a complete ban on advertising that is targeted using protected data such as sexual orientation, ethnicity, or religion and targeted advertising aimed at minors.

**How does the EU protect children on online platforms?**

While the EU already has some rules to protect children online, such as those found in the Audiovisual Media Services Directive ([https://digital-strategy.ec.europa.eu/en/policies/avmsd-protection-minors](https://digital-strategy.ec.europa.eu/en/policies/avmsd-protection-minors)), the Digital Services Act (DSA) introduces specific obligations for platforms.

Among other obligations, the DSA requires intermediary services that are primarily directed or used by minors to make efforts to ensure their terms and conditions are easily understandable by minors.

Moreover, online platforms used by minors should:

- design their interface with the highest level of privacy, security and safety for minors or participate in codes of conduct for protecting minors;
- consider the best practices and available guidance, such as the new European strategy for a better internet for kids ([https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids](https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids)) (BIK+);
- not present advertisements to minors based on profiling.

Very large online platforms and search engines (VLOPs and VLOSEs) must make additional efforts to protect minors.

This includes making sure their risk assessment covers fundamental rights, which include the rights of the child. They should assess how easy it is for children and adolescents to understand how their service works and possible exposures to content that could impair their physical or mental wellbeing, or moral development.

**Enforcement**

**Who enforces the DSA?**

The supervision of the rules will be shared between the Commission – primarily responsible for VLOPs and VLOSEs – and Member States, responsible for other platforms and search engines according to where they are established.

The Commission will have the same supervisory powers as it has under current anti-trust rules, including investigatory powers and the ability to impose fines of up to 6% of global revenue.
Member States will be required to designate competent authorities – referred to as Digital Services Coordinators – by 17 February 2024 to supervise compliance of the services established in their jurisdiction, and to participate in the EU cooperation mechanism.

**What is a Digital Service Coordinator?**

A Digital Service Coordinator (DSC) is an authority in charge of the application and enforcement of the DSA in each Member State. They must be designated by Member States by 17 February 2023.

DSCs will contribute to monitoring the enforcement of the DSA together with the Commission. They will have powers to request access to VLOPs/VLOSEs data, order inspections and impose fines in the event of an infringement. They will also be responsible for certifying “trusted flaggers” and out-of-court dispute settlement bodies.

**What is a trusted flagger?**

Trusted flaggers have particular expertise and competence for the purposes of detecting, identifying, and notifying illegal content and are independent from online platforms. Online platforms must ensure that notices submitted by trusted flaggers are given priority and are processed timely.

Under the Digital Services Act, a trusted flagger is a status awarded by the Digital Service Coordinator in the Member State in which the applicant for trusted flagger resides.

To be successful, the applicant must:

- Have particular expertise and competence for the purposes of detecting, identifying, and notifying illegal content;
- Be independent from any provider of online platforms;
- Carry out their activities for the purposes of submitting notices of illegal content diligently, accurately, and objectively.

**How do I apply to become a trusted flagger?**

The status of ‘trusted flagger’ will be awarded by the Digital Services Coordinator of the Member State in which the applicant is established, provided that the applying entity meets all of the conditions set out in the Regulation.

Digital Services Coordinators will start operating at the latest on 17 February 2024. We advise you to monitor developments in the Member State of your establishment ahead of this date to find information about the detailed procedure, which will be regulated at national level.

Please note that only entities with an establishment in the EU may apply for the ‘trusted flagger’ status under the DSA.

**What kind of arrangements will help ensure the independence of Digital Services Coordinators in regard to platforms?**

The DSA sets out a high standard for the independence of national regulators. It includes explicit requirements for independence when designating Digital Services Coordinators in Member States. Member States will need to ensure their Digital Services Coordinator has adequate financial, technical, and human resources to carry out their tasks.

The Digital Services Coordinators should remain fully independent in their decision-making and not seek instructions from their governments or other bodies, particularly online platforms.

**Can the DSA censor platforms/impact of freedom of expression?**

Under the DSA, very large online platforms or very large online search engines have to perform an assessment of the risks stemming from their services. This includes disinformation or election manipulation, cyber violence against women, or harms to minors online. They then have to take corresponding risk mitigating measures.

There may be times when there is doubt on the ability of a very large online platform or search engine to address risks to
The Commission’s investigatory powers include a possibility to send requests for information, a power to conduct interviews or inspections as well as enforcement related powers, such as imposing additional measures, fines, or periodic penalty payments.

These powers can only be used in justified cases of ensuring compliance with the DSA and only to the extent this is necessary and proportionate. All Commission decisions are subject to judicial redress before the Court of Justice of the EU.

In the event of a crisis, the national digital service coordinator, or the Commission, can adopt interim measures. However, such measures should be considered as a last resort. The Commission values freedom of expression and information as key pillars in our democracies. Therefore, any measures cannot go beyond what is necessary to prevent serious harms and should be limited in time, ceasing to apply once the full range of evidence has been collected.

In addition, Article 8 of the DSA explicitly specifies that it is prohibited to impose general monitoring obligations on online platform providers.