

Contribution ID: 9ee7d4aa-6515-49be-89cf-3c5edbfac371

Date: 08/09/2020 17:57:30

# Digital Services Act package: open public consultation

Fields marked with \* are mandatory.

---

## Introduction

---

The Commission recently announced ([https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020\\_en\\_4.pdf](https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf)) a Digital Services Act package with two main pillars:

- first, a proposal of new and revised rules to deepen the Single Market for Digital Services, by increasing and harmonising the responsibilities of online platforms and information service providers and reinforce the oversight over platforms' content policies in the EU;
- second, ex ante rules to ensure that markets characterised by large platforms with significant network effects acting as gatekeepers, remain fair and contestable for innovators, businesses, and new market entrants.

## This consultation

The Commission is initiating the present open public consultation as part of its evidence-gathering exercise, in order to identify issues that may require intervention through the Digital Services Act, as well as additional topics related to the environment of digital services and online platforms, which will be further analysed in view of possible upcoming initiatives, should the issues identified require a regulatory intervention.

The consultation contains 6 modules (you can respond to as many as you like):

1. **How to effectively keep users safer online?**
2. **Reviewing the liability regime of digital services acting as intermediaries?**
3. **What issues derive from the gatekeeper power of digital platforms?**
4. **Other emerging issues and opportunities, including online advertising and smart contracts**
5. **How to address challenges around the situation of self-employed individuals offering services through online platforms?**
6. **What governance for reinforcing the Single Market for digital services?**

## Digital services and other terms used in the questionnaire

The questionnaire refers to **digital services** (or 'information society services', within the meaning of the E-Commerce Directive), as 'services provided through electronic means, at a distance, at

the request of the user'. It also refers more narrowly to a subset of digital services here termed **online intermediary services**. By this we mean services such as internet access providers, cloud services, online platforms, messaging services, etc., i.e. services that generally transport or intermediate content, goods or services made available by third parties.

Parts of the questionnaire specifically focus on **online platforms** – such as e-commerce marketplaces, search engines, app stores, online travel and accommodation platforms or mobility platforms and other collaborative economy platforms, etc.

Other terms and other technical concepts are explained in a glossary (<https://ec.europa.eu/eusurvey/files/b77fbb2f-fd46-4dfd-8fc9-ecea1353266a/0da338ef-fea6-4e44-b2ef-a665a91604cf>).

## How to respond

Make sure to **save your draft** regularly as you fill in the questionnaire.

You can break off and return to finish it at any time.

At the end, you will also be able to upload a document or add other issues not covered in detail in the questionnaire.

## Deadline for responses

8 September 2020.

## Languages

You can submit your response in any official EU language.

The questionnaire is available in 23 of the EU's official languages. You can switch languages from the menu at the top of the page.

---

## About you

---

\*1 Language of my contribution

\*2 I am giving my contribution as

\*3 First name

\*4 Surname

Pielemeier

\*5 Email (this won't be published)

\*7 Organisation name

255 character(s) maximum

Global Network Initiative

\*8 Organisation size

Micro (1 to 9 employees)

9 What is the annual turnover of your company?

- <=€2m
- <=€10m
- <= €50m
- Over €50m

10 Are you self-employed and offering services through an online platform?

- Yes
- No

16 Does your organisation play a role in:

- Flagging illegal activities or information to online intermediaries for removal
- Fact checking and/or cooperating with online platforms for tackling harmful (but not illegal) behaviours
- Representing fundamental rights in the digital environment
- Representing consumer rights in the digital environment
- Representing rights of victims of illegal activities online
- Representing interests of providers of services intermediated by online platforms
- Other

17 Is your organisation a

- Law enforcement authority, in a Member State of the EU
- Government, administrative or other public authority, other than law enforcement, in a Member State of the EU
- Other, independent authority, in a Member State of the EU
- EU-level authority
- International level authority, other than at EU level
- Other

18 Is your business established in the EU?

- Yes  
 No

## 20 Transparency register number

*255 character(s) maximum*

Check if your organisation is on the transparency register (<http://ec.europa.eu/transparencyregister/public/homePage.do?redir=false&locale=en>). It's a voluntary database for organisations seeking to influence EU decision-making.

602889028780-88

## \*21 Country of origin

Please add your country of origin, or that of your organisation.

United States

## \*22 Publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

**Anonymous**

Only your type of respondent, country of origin and contribution will be published. All other personal details (name, organisation name and size, transparency register number) will not be published.

**Public**

Your personal details (name, organisation name and size, transparency register number, country of origin) will be published with your contribution.

I agree with the personal data protection provisions ([https://ec.europa.eu/info/law/better-regulation/specific-privacy-statement\\_en](https://ec.europa.eu/info/law/better-regulation/specific-privacy-statement_en))

---

## I. How to effectively keep users safer online?

---

This module of the questionnaire is structured into several subsections:

**First**, it seeks evidence, experience, and data from the perspective of different stakeholders regarding illegal activities online, as defined by national and EU law. This includes the availability online of illegal goods (e.g. dangerous products, counterfeit goods, prohibited and restricted goods, protected wildlife, pet trafficking, illegal medicines, misleading offerings of food supplements), content (e.g. illegal hate speech, child sexual abuse material, content that infringes intellectual property rights), and services, or practices that infringe consumer law (such as scams, misleading advertising, exhortation to purchase made to children) online. It covers all types of illegal activities, both as regards criminal law and civil law.

It then asks you about other activities online that are not necessarily illegal but could cause harm to users, such as the spread of online disinformation or harmful content to minors.

It also seeks facts and informed views on the potential risks of erroneous removal of legitimate content. It also asks you about the transparency and accountability of measures taken by digital services and online platforms in particular in intermediating users' access to their content and enabling oversight by third parties. Respondents might also be interested in related questions in the module of the consultation focusing on online advertising.

**Second**, it explores proportionate and appropriate responsibilities and obligations that could be required from online intermediaries, in particular online platforms, in addressing the set of issues discussed in the first subsection.

This module does not address the liability regime for online intermediaries, which is further explored in the next module of the consultation.

---

## **1. Main issues and experiences**

---

### **A. Experiences and data on illegal activities online**

#### **Illegal goods**

1 Have you ever come across illegal goods on online platforms (e.g. a counterfeit product, prohibited and restricted goods, protected wildlife, pet trafficking, illegal medicines, misleading offerings of food supplements)?

- No, never
- Yes, once
- Yes, several times
- I don't know

3 Please specify.

*3,000 character(s) maximum*

4 How easy was it for you to find information on where you could report the illegal good?

Please rate from 1 star (very difficult) to 5 stars (very easy)



5 How easy was it for you to report the illegal good?

Please rate from 1 star (very difficult) to 5 stars (very easy)



6 How satisfied were you with the procedure following your report?

Please rate from 1 star (very dissatisfied) to 5 stars (very satisfied)



7 Are you aware of the action taken following your report?

- Yes
- No

8 Please explain

*3,000 character(s) maximum*

9 In your experience, were such goods more easily accessible online since the outbreak of COVID-19?

- No, I do not think so
- Yes, I came across illegal offerings more frequently
- I don't know

10 What good practices can you point to in handling the availability of illegal goods online since the start of the COVID-19 outbreak?

*5,000 character(s) maximum*

## Illegal content

11 Did you ever come across illegal content online (for example illegal incitement to violence, hatred or discrimination on any protected grounds such as race, ethnicity, gender or sexual orientation; child sexual abuse material; terrorist propaganda; defamation; content that infringes intellectual property rights, consumer law infringements)?

- No, never
- Yes, once
- Yes, several times
- I don't know

18 How has the dissemination of illegal content changed since the outbreak of COVID-19? Please explain.

*3,000 character(s) maximum*

19 What good practices can you point to in handling the dissemination of illegal content online since the outbreak of COVID-19?

*3,000 character(s) maximum*

20 What actions do online platforms take to minimise risks for consumers to be exposed to scams and other unfair practices (e.g. misleading advertising, exhortation to purchase made to children)?

*3,000 character(s) maximum*

21 Do you consider these measures appropriate?

- Yes
- No
- I don't know

22 Please explain.

*3,000 character(s) maximum*

## B. Transparency

1 If your content or offering of goods and services was ever removed or blocked from an online platform, were you informed by the platform?

- Yes, I was informed before the action was taken
- Yes, I was informed afterwards
- Yes, but not on every occasion / not by all the platforms
- No, I was never informed
- I don't know

3 Please explain.

*3,000 character(s) maximum*

4 If you provided a notice to a digital service asking for the removal or disabling of access to such content or offering of goods or services, were you informed about the follow-up to the request?

- Yes, I was informed
- Yes, but not on every occasion / not by all platforms
- No, I was never informed
- I don't know

5 When content is recommended to you - such as products to purchase on a platform, or videos to watch, articles to read, users to follow - are you able to obtain enough information on why such content has been recommended to you? Please explain.

*3,000 character(s) maximum*

## C. Activities that could cause harm but are not, in themselves, illegal

1 In your experience, are children adequately protected online from harmful behaviour, such as grooming and bullying, or inappropriate content?

*3,000 character(s) maximum*

2 To what extent do you agree with the following statements related to online disinformation?

	F u l l y  a g r e e	S o m e w h a t a g r e e	N e i t h e r  a g r e e  n o t  d i s a g r e e	S o m e w h a t d i s a g r e e	F u l l y  d i s a g r e e	I  d o n' t k n o w  / N o  r e p l y

Online platforms can easily be manipulated by foreign governments or other coordinated groups to spread divisive messages	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
To protect freedom of expression online, diverse voices should be heard	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Disinformation is spread by manipulating algorithmic processes on online platforms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online platforms can be trusted that their internal practices sufficiently guarantee democratic integrity, pluralism, non-discrimination, tolerance, justice, solidarity and gender equality.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3 Please explain.

*3,000 character(s) maximum*

4 In your personal experience, how has the spread of harmful (but not illegal) activities online changed since the outbreak of COVID-19? Please explain.

*3,000 character(s) maximum*

5 What good practices can you point to in tackling such harmful activities since the outbreak of COVID-19?

*3,000 character(s) maximum*

## D. Experiences and data on erroneous removals

This section covers situation where content, goods or services offered online may be removed erroneously contrary to situations where such a removal may be justified due to for example illegal nature of such content, good or service (see sections of this questionnaire above).

1 Are you aware of evidence on the scale and impact of erroneous removals of content, goods, services, or banning of accounts online? Are there particular experiences you could share?

*5,000 character(s) maximum*

***The following questions are targeted at organisations.***

***Individuals responding to the consultation are invited to go to section 2 here below on responsibilities for online platforms and other digital services***



3 What is your experience in flagging content, or offerings of goods or services you deemed illegal to online platforms and/or other types of online intermediary services? Please explain in what capacity and through what means you flag content.

*3,000 character(s) maximum*

4 If applicable, what costs does your organisation incur in such activities?

*3,000 character(s) maximum*

5 Have you encountered any issues, in particular, as regards illegal content or goods accessible from the EU but intermediated by services established in third countries? If yes, how have you dealt with these?

*3,000 character(s) maximum*

6 If part of your activity is to send notifications or orders for removing illegal content or goods or services made available through online intermediary services, or taking other actions in relation to content, goods or services, please explain whether you report on your activities and their outcomes:

- Yes, through regular transparency reports
- Yes, through reports to a supervising authority
- Yes, upon requests to public information
- Yes, through other means. Please explain
- No, no such reporting is done

8 Does your organisation access any data or information from online platforms?

- Yes, data regularly reported by the platform, as requested by law
- Yes, specific data, requested as a competent authority
- Yes, through bilateral or special partnerships
- On the basis of a contractual agreement with the platform
- Yes, generally available transparency reports
- Yes, through generally available APIs (application programme interfaces)
- Yes, through web scraping or other independent web data extraction approaches
- Yes, because users made use of their right to port personal data
- Yes, other. Please specify in the text box below
- No

10 What sources do you use to obtain information about users of online platforms and other digital services – such as sellers of products online, service providers, website holders or providers of content online? For what purpose do you seek this information?

*3,000 character(s) maximum*

11 Do you use WHOIS information about the registration of domain names and related information?

- Yes
- No

I don't know

13 How valuable is this information for you?

Please rate from 1 star (not particularly important) to 5 (extremely important)



14 Do you use or are you aware of alternative sources of such data? Please explain.

*3,000 character(s) maximum*

---

***The following questions are targeted at online intermediaries.***

---

## **A. Measures taken against illegal goods, services and content online shared by users**

1 What systems, if any, do you have in place for addressing illegal activities conducted by the users of your service (sale of illegal goods -e.g. a counterfeit product, an unsafe product, prohibited and restricted goods, wildlife and pet trafficking - dissemination of illegal content or illegal provision of services)?

- A notice-and-action system for users to report illegal activities
- A dedicated channel through which authorities report illegal activities
- Cooperation with trusted organisations who report illegal activities, following a fast-track assessment of the notification
- A system for the identification of professional users ("know your customer")
- A system for penalising users who are repeat offenders
- A system for informing consumers that they have purchased an illegal good, once you become aware of this
- Multi-lingual moderation teams
- Automated systems for detecting illegal activities. Please specify the detection system and the type of illegal content it is used for
- Other systems. Please specify in the text box below
- No system in place

2 Please explain.

*5,000 character(s) maximum*

3 What issues have you encountered in operating these systems?

*5,000 character(s) maximum*

4 On your marketplace (if applicable), do you have specific policies or measures for the identification of sellers established outside the European Union ?

- Yes
- No

5 Please quantify, to the extent possible, the costs of the measures related to 'notice-and-action' or other measures for the reporting and removal of different types of illegal goods, services and content, as relevant.

*5,000 character(s) maximum*

6 Please provide information and figures on the amount of different types of illegal content, services and goods notified, detected, removed, reinstated and on the number or complaints received from users. Please explain and/or link to publicly reported information if you publish this in regular transparency reports.

*5,000 character(s) maximum*

7 Do you have in place measures for detecting and reporting the incidence of suspicious behaviour (i.e. behaviour that could lead to criminal acts such as acquiring materials for such acts)?

*3,000 character(s) maximum*

---

## **B. Measures against other types of activities that might be harmful but are not, in themselves, illegal**

1 Do your terms and conditions and/or terms of service ban activities such as:

- Spread of political disinformation in election periods?
- Other types of coordinated disinformation e.g. in health crisis?
- Harmful content for children?
- Online grooming, bullying?
- Harmful content for other vulnerable persons?
- Content which is harmful to women?
- Hatred, violence and insults (other than illegal hate speech)?
- Other activities which are not illegal per se but could be considered harmful?

2 Please explain your policy.

*5,000 character(s) maximum*

3 Do you have a system in place for reporting such activities? What actions do they trigger?

*3,000 character(s) maximum*

4 What other actions do you take? Please explain for each type of behaviour considered.

*5,000 character(s) maximum*

5 Please quantify, to the extent possible, the costs related to such measures.

*5,000 character(s) maximum*

6 Do you have specific policies in place to protect minors from harmful behaviours such as online grooming or bullying?

- Yes  
 No

7 Please explain.

*3,000 character(s) maximum*

## C. Measures for protecting legal content goods and services

1 Does your organisation maintain an internal complaint and redress mechanism to your users for instances where their content might be erroneously removed, or their accounts blocked?

- Yes  
 No

2 What action do you take when a user disputes the removal of their goods or content or services, or restrictions on their account? Is the content/good reinstated?

*5,000 character(s) maximum*

3 What are the quality standards and control mechanism you have in place for the automated detection or removal tools you are using for e.g. content, goods, services, user accounts or bots?

*3,000 character(s) maximum*

4 Do you have an independent oversight mechanism in place for the enforcement of your content policies?

- Yes  
 No

5 Please explain.

*5,000 character(s) maximum*

## D. Transparency and cooperation

1 Do you actively provide the following information:

- Information to users when their good or content is removed, blocked or demoted  
 Information to notice providers about the follow-up on their report  
 Information to buyers of a product which has then been removed as being illegal

2 Do you publish transparency reports on your content moderation policy?

- Yes  
 No

3 Do the reports include information on:

- Number of takedowns and account suspensions following enforcement of your terms of service?  
 Number of takedowns following a legality assessment?  
 Notices received from third parties?  
 Referrals from authorities for violations of your terms of service?  
 Removal requests from authorities for illegal activities?  
 Number of complaints against removal decisions?  
 Number of reinstated content?  
 Other, please specify in the text box below

4 Please explain.

*5,000 character(s) maximum*

5 What information is available on the automated tools you use for identification of illegal content, goods or services and their performance, if applicable? Who has access to this information? In what formats?

*5,000 character(s) maximum*

6 How can third parties access data related to your digital service and under what conditions?

- Contractual conditions  
 Special partnerships  
 Available APIs (application programming interfaces) for data access  
 Reported, aggregated information through reports  
 Portability at the request of users towards a different service  
 At the direct request of a competent authority  
 Regular reporting to a competent authority  
 Other means. Please specify

7 Please explain or give references for the different cases of data sharing and explain your policy on the different purposes for which data is shared.

*5,000 character(s) maximum*

---

***The following questions are open for all respondents.***

---

## **2. Clarifying responsibilities for online platforms and other digital services**

1 What responsibilities (i.e. legal obligations) should be imposed on online platforms and under what conditions?

Should such measures be taken, in your view, by all online platforms, or only by specific ones (e.g. depending on their size, capability, extent of risks of exposure to illegal activities conducted by their users)? If you consider that some measures should only be taken by large online platforms, please identify which would these measures be.

	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)	Yes, only by larger online platforms	Yes, only platforms at particular risk of exposure to illegal activities by their users	Such measures should not be required by law
Maintain an effective 'notice and action' system for reporting illegal goods or content	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Maintain a system for assessing the risk of exposure to illegal goods or content	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Have content moderation teams, appropriately trained and resourced	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Systematically respond to requests from law enforcement authorities	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cooperate with national authorities and law enforcement, in accordance with clear procedures	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cooperate with trusted organisations with proven expertise that can report illegal activities for fast analysis ('trusted flaggers')	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Detect illegal content, goods or services	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
In particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Request professional users to identify themselves clearly ('know your customer' policy)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Provide technical means allowing professional users to comply with their obligations (e.g. enable them to publish on the platform the pre-contractual information consumers need to receive in accordance with applicable consumer law)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Inform consumers when they become aware of product recalls or sales of illegal goods	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cooperate with other online platforms for exchanging best practices, sharing information or tools to tackle illegal activities	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Be transparent about their content policies, measures and their effects	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Maintain an effective 'counter-notice' system for users whose goods or content is removed to dispute erroneous decisions	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other. Please specify	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 2 Please elaborate, if you wish to further explain your choices.

*5,000 character(s) maximum*

The notion of online platforms provided in the European Commission glossary of the public consultation refers to a variety of hosting service providers with a broad range of different features. This makes it difficult to properly respond to the table above and link certain measures to a specific group or sub-group of online platforms. Responsibilities beyond current provisions applicable to any hosting service provider should be legally required only in a targeted way to ensure legal clarity and avoid infringement on fundamental rights and freedoms.

## 3 What information would be, in your view, necessary and sufficient for users and third parties to send to an online platform in order to notify an illegal activity (sales of illegal goods, offering of services or sharing illegal content) conducted by a user of the service?

- Precise location: e.g. URL
- Precise reason why the activity is considered illegal
- Description of the activity
- Identity of the person or organisation sending the notification. Please explain under what conditions such information is necessary:
- Other, please specify

## 4 Please explain

*3,000 character(s) maximum*

In general, the notification procedure should be easily accessible, reliable, and user-friendly. Non-experts should be able to make notifications, but still provide sufficient information, including stated reason/explanation and supporting evidence, in order to discourage false notifications. Additionally, "description of the activity" could be more specific, and include the "particular activity that is alleged to be illegal."

We believe that some disclosure of identity is important for the sake of tackling potential misuse of notice mechanisms (e.g. attempts to "silence other users"), but it should remain voluntary. This should be continuously complemented by anonymous reporting tools provided by independent third parties. The default should be for notifiers to identify themselves, since their identity can provide relevant contextual information that can help online platforms evaluate their notices. This identifying information may in fact be necessary to establish the basis for certain types of claims, for instance in the context of defamation or copyright. Even outside of those contexts, complete anonymity of notifiers can frustrate efforts to obtain additional information, allow counter-notice, punish bad faith notices, and provide public transparency. However, there are also valid reasons to protect the identity of certain notifiers and the DSA should proactively identify ways in which individuals can make notifications while protecting their identity. For instance, it may be possible for certain validated organizations to submit notices on behalf of individuals in such circumstances.

Additionally, in contrast to the fragmented system currently in place, the notice and action procedure should be uniform across the EU. A harmonized EU system should still be flexible, and not overly prescriptive to account for the changes in platform use and technology. As part of this common system, third parties should not "notify illegal activity" since they cannot adjudicate legality. Instead, they should notify the platform of content that they believe to be illegal (i.e. an "allegation" of illegality) and/or violates the online platform's terms of service/community guidelines.

## 5 How should the reappearance of illegal content, goods or services be addressed, in your view? What approaches are effective and proportionate?

*5,000 character(s) maximum*

Online platforms should be allowed to identify accounts that repeatedly post illegal content and sanction them according to their terms of service. They should also be encouraged to use hash databases and other tools to flag content that appears identical to content that has previously been adjudicated to be illegal or contrary to their terms of service. In certain limited circumstances, such as Child Sexual Abuse Material (CSAM), where automated detection is highly reliable and there are limited or no "fair use" or other appropriate exceptions to illegality, online platforms should be encouraged to remove content that is identified with a high degree of likelihood as having been previously adjudicated to be illegal or contrary to their terms of service. Outside of these limited circumstances, the DSA should uphold and reiterate the prohibition on general monitoring requirements and make clear that platforms are not required to automatically remove similar but not identical content or rely exclusively on automated filtering technology to identify and remove illegal content. For more on this topic, please see our response to Question 6 in this section below.



6 Where automated tools are used to detect illegal content, goods or services, what opportunities and risks does their use present as regards different types of illegal activities and the particularities of the different types of tools?

*3,000 character(s) maximum*

Many platforms are turning to automation to scale their content moderation practices. When used appropriately, these tools can help platforms identify illegal and otherwise inappropriate content/behavior. While this may be appropriate and reliable in some cases, it is not for others. Artificial Intelligence (AI) has supplemented human oversight and helped scale the identification of harmful content, but it also poses several risks to free expression. For one, AI-enabled tools are more or less successful at identifying certain forms of images, such as CSAM material, but the chances for error and over-removal increases when the infringing content is less easily defined, and more nuanced. AI-enabled tools have proven less reliable, and in some instances completely inadequate, where adjudication of content relies on context. For instance, an AI-enabled tool trained on hate speech terms may mistakenly flag a satirical comment as "hate speech."

In other circumstances, important contextual information that allows for accurate detection of illegal content. For instance, fair use exceptions to copyright or journalistic coverage of violence. As such, companies must use automated tools very cautiously. Likewise, legislators should not impose general monitoring obligations and should encourage proper safeguards, including mandating human oversight, transparency obligations, as well as robust and accessible appeals mechanisms so that legitimate content can be quickly reinstated.

7 How should the spread of illegal goods, services or content across multiple platforms and services be addressed? Are there specific provisions necessary for addressing risks brought by:

- a. Digital services established outside of the Union?
- b. Sellers established outside of the Union, who reach EU consumers through online platforms?

*3,000 character(s) maximum*

It is worth noting that most of the digital services that may be relevant to the DSA are already required to establish and appoint a local representative in line with other, existing EU regulations. Separately, any approach to services established or illegal content hosted outside of the Union must be developed carefully, in a manner consistent with the international human rights principles of necessity and proportionality. The GNI has raised concerns about recent Court of Justice of the European Union (CJEU) and other foreign court decisions that appear to open the door for Member State authorities to require content be removed or restricted globally. Such global removal orders are unlikely to be consistent with the above mentioned principles in most circumstances.

Given that EU law and jurisprudence differ in certain ways from speech-related laws in other jurisdictions, efforts to address content that is deemed illegal in the Union should avoid or otherwise minimize any impacts on the availability of the same content outside the Union. In this way, the Union can minimize conflicts of law, respect the international law principle of comity, and avoid creating precedents that could be used by other countries to restrict the availability of content that is legal, or even protected, under EU law.

8 What would be appropriate and proportionate measures for digital services acting as online intermediaries, other than online platforms, to take – e.g. other types of hosting services, such as web hosts, or services deeper in the internet stack, like cloud infrastructure services, content distribution services, DNS services, etc.?

*5,000 character(s) maximum*

The DSA should clearly define the services which are appropriately positioned to address the specific concern at hand. There should also not be a 'one size fits all' solution to regulate the diverse intermediaries. The capabilities of a DNS provider or cloud infrastructure service will necessarily be different from a social media platform. The former do not have the same degree of insight into or control over the content on their services as the latter. As a general rule, the further removed a service is from the Internet's application layer (in other words, the deeper within the internet stack a service is located), the less effectively and/or proportionally they are able to address specific content. As such, the DSA should be structured to avoid or minimize the extent to which legal liability and illegal content/behavior-related demands are imposed on such services.

9 What should be the rights and responsibilities of other entities, such as authorities, or interested third-parties such as civil society organisations or equality bodies in contributing to tackle illegal activities online?

*5,000 character(s) maximum*

It is important to distinguish here between the roles of public authorities and private bodies. Certain public authorities can and should be allowed and encouraged to develop mechanisms for identifying and assessing potentially illegal content/activities online. Agencies or authorities who are vested with this responsibility should be clearly identified and authorized, and relevant procedures and evidentiary thresholds should be carefully set out in publicly available laws. Where such public authorities determine online content/activity is illegal based on these procedures, they may choose to notify online platforms who can then determine whether it violates their terms of service and act accordingly. Failure to act in response to specific notifications based on terms-of-service violations must not be a basis for intermediary liability or otherwise punishable under the law.

Public authorities may also or instead choose to take their concerns to duly authorized, independent, public adjudicators. If such an adjudicator finds the content/activity to be illegal, it may notify relevant online platforms, at which point they should be deemed to have "actual knowledge" for the purposes of liability and act accordingly. The law may also clearly identify circumstances and procedures for emergency notices by public authorities, which must be addressed by online platforms in a timely manner. These instances should be rare and must be followed by timely review by an independent adjudicator.

Independent third parties, such as users or civil society organizations, should be allowed and empowered to notify both online platforms and public authorities when they believe illegal content/activity exists online. The procedures and requirements for making such notifications should be clear and accessible. Online platforms and relevant public authorities should be allowed to establish direct relationships with certain groups of reliable notifiers that have demonstrated expertise and credibility and to effectively prioritize notices from such groups (such relationships are sometimes referred to as "trusted flaggers/notifiers"), provided that the criteria for, establishment of, and operational details of such relationships are transparent and non-discriminatory. As with notifications from public authorities that have not been reviewed by an independent adjudicator, the law should make clear that online platforms are not bound to comply with private notifications and that failure to take action cannot be a basis for liability.

Whenever content/activity is alleged to be illegal, unless certain exceptional circumstances set out in law are met, the individuals or entities responsible for the content/activity alleged to be illegal must be provided timely notice and an opportunity to respond. When content/activity is removed or otherwise sanctioned pursuant to either an intermediary's terms of service or a governmental order, persons impacted by such decisions must be given an opportunity to appeal. The fact of and reasoning behind such a determination should be made public. In other words, public authorities should make removal orders in writing and, absent exceptional circumstances, allow intermediaries to publish them. Governments and online platforms should also be required to provide periodic transparency reports that reveal the number, type of, and resulting decisions associated with referrals or orders related to content/activity alleged or adjudicated to be illegal. For more on our views on transparency, see our response to Question 4 in the Governance and Enforcement section.

**10 What would be, in your view, appropriate and proportionate measures for online platforms to take in relation to activities or content which might cause harm but are not necessarily illegal?**

**5,000 character(s) maximum**

Principles of legality and proportionality require clear understandings of what is legal and illegal. It is essential that the DSA clearly distinguish between 'illegal' and 'legal but harmful' content/activity. The DSA should not obligate online platforms to remove legal content or otherwise violate free expression rights.

In light of their recent actions and continuing public pressure, online platforms are likely to continue taking voluntary measures to sanction content that violates their terms of service. In order to ensure that such voluntary actions are taken in a fair and non-discriminatory manner, the DSA could require detailed reporting/transparency criteria for such decisions and require that covered online platforms' procedures for notification and adjudication meet due process requirements, including accessible and timely opportunities for appeal. These rules should be sufficiently clear for users, so they can accurately abide by them as well as take advantage of their rights.

One important and potentially concerning trend is the increased reliance by online platforms on machine learning-enabled content filtering tools, which some platforms are increasingly turning to identify, and in some instances remove, certain forms of content at scale. While such tools may be capable of identifying certain content/activity with a high degree of accuracy in certain narrow circumstances (e.g., child sexual abuse images or content/activity that has previously been properly actioned and is being re-posted), such tools are much less capable of accurately discerning other types of speech. Over-reliance on such tools can therefore result in over-broad removal of legal content/activity. The DSA should not explicitly or implicitly require or incentivize online platforms to rely exclusively on content filtering tools, without effective human review. Requiring transparency about the design, use, and oversight of such tools, as well as robust and accessible appeals mechanisms so that legitimate content can be quickly reinstated, will help address concerns that they may lead to unnecessary or disproportionate impacts on free expression.

**11 In particular, are there specific measures you would find appropriate and proportionate for online platforms to take in relation to potentially harmful activities or content concerning minors? Please explain.**

**5,000 character(s) maximum**

Certain types of harmful content concerning minors are already illegal (i.e. CSAM) and online platforms are under strict obligations to remove it in most EU member states. However, other types of content, such as bullying or encouraging eating disorders, are harmful, but not illegal. A study by the IMCO committee recommends a co-regulatory approach to protect minors from harmful content. Online platforms and authorities could jointly promote the use of parental controls and rating systems. The AVMSD already requires video service providers "to take appropriate measures to protect minors from content which may impair their physical, mental, or moral development." In addition, most platforms impose minimum age requirements for accessing their services, and public authorities can facilitate advice and tools for better enforcing these rules. Processes based on co- and self-regulation can play an important role in this regard.

12 Please rate the necessity of the following measures for addressing the spread of disinformation online. Please rate from 1 (not at all necessary) to 5 (essential) each option below.

	1 (not at all necessary)	2	3 (neutral)	4	5 (essential)	I don't know / No answer
Transparently inform consumers about political advertising and sponsored content, in particular during election periods	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with user complaints	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Tackle the use of fake-accounts, fake engagements, bots and inauthentic users behaviour aimed at amplifying false or misleading narratives	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Transparency tools and secure access to platform data for trusted researchers in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Transparency tools and secure access to platform data for authorities in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Adapted risk assessments and mitigation strategies undertaken by online platforms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Ensure effective access and visibility of a variety of authentic and professional journalistic sources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Auditing systems for platform actions and risk assessments	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Regulatory oversight and auditing competence over platforms' actions and risk assessments, including on sufficient resources and staff, and responsible examination of metrics and capacities related to fake accounts and their impact on the manipulation and amplification of disinformation.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Other (please specify)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
------------------------	-----------------------	-----------------------	-----------------------	-----------------------	----------------------------------	-----------------------

### 13 Please specify

*3,000 character(s) maximum*

Efforts to better educate and inform the public at large and online platform users specifically about disinformation and how to identify and mitigate its impacts. This can and should be integrated into broader public education, critical thinking, and digital literacy efforts.

In addition to the efforts referred to above to address "inauthentic" users and/or behavior, it is also worth noting that such measures will not address similar challenges that can be presented by "authentic" users who may amplify false or misleading narratives. Separately, while transparency and access to platform data can serve to draw learnings from and validate efforts to address illegal content and inauthentic behavior, it can also raise serious privacy concerns. This is especially the case with regard to additional access to content and data by public authorities. These are not insurmountable but must be addressed with significant safeguards. Finally, while there is much value to be gained from promoting credible, authoritative information and sources, including professional journalists, the processes and standards for determining who meets these criteria must be very carefully thought through and developed in a manner that will reinforce their legitimacy.

### 14 In special cases, where crises emerge and involve systemic threats to society, such as a health pandemic, and fast-spread of illegal and harmful activities online, what are, in your view, the appropriate cooperation mechanisms between digital services and authorities?

*3,000 character(s) maximum*

We support concerted action from all relevant stakeholders to swiftly address systemic threats to society. Digital service providers require legal certainty when taking specific actions in response to systemic threats. Potential obligations related to such contexts should be clearly and strictly limited in order to avoid misuse of emergency powers.

In situations of crisis, co-regulatory approaches may help provide appropriate cooperation mechanisms that can be timely and effective, while ensuring that crisis response measures remain necessary and proportionate. It is important that crises or emergency situations should not justify violating people's fundamental rights. Clear criteria should be established for when a crisis or emergency may be declared, what, if any, implications this may have for online platforms and/or other intermediaries, how any resulting actions may be carried out, and when the crisis or emergency should be deemed to have concluded. Any crisis cooperation mechanisms should be as transparent as possible and ideally should include participation of relevant civil society actors.

### 15 What would be effective measures service providers should take, in your view, for protecting the freedom of expression of their users? Please rate from 1 (not at all necessary) to 5 (essential).

	1 (not at all necessary)	2	3 (neutral)	4	5 (essential)	I don't know / No answer
High standards of transparency on their terms of service and removal decisions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Diligence in assessing the content notified to them for removal or blocking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Maintaining an effective complaint and redress mechanism	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Diligence in informing users whose content/goods/services was removed or blocked or whose accounts are threatened to be suspended	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
High accuracy and diligent control mechanisms, including human oversight, when automated tools are deployed for detecting, removing or demoting content or suspending users' accounts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Enabling third party insight – e.g. by academics – of main content moderation systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Other. Please specify	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

16 Please explain.

*3,000 character(s) maximum*

Under "Other": 1) providing accessible and effective remedy to users who wish to appeal content/behavior-related decisions; 2) ensuring that content moderation is carried out in a manner that is consistent and non-discriminatory; 3) An obligation to give users control over their data and content. For instance, users should be able to opt out of or control the collection of data used for the purposes of micro-targeted advertising and personalized content, as well as the filters that are used to rank/prioritize what content they are shown.

Also, see response to Q. 10 above.

The DSA should focus on the removal of content that has been adjudicated illegal by a competent, independent authority. Imposing blocking injunctions on internet access providers should always be a last resort and the DSA should clearly differentiate the requisite procedures and expectations that apply to removal and blocking orders respectively.

**17 Are there other concerns and mechanisms to address risks to other fundamental rights such as freedom of assembly, non-discrimination, gender equality, freedom to conduct a business, or rights of the child? How could these be addressed?**

*5,000 character(s) maximum*

While the EU has privacy legislation in place, it should still be cognizant of how it balances obligations related to illegal content with privacy rights. Legislators should be careful to not impose rules or conditions, including "tracing" requirements or general monitoring obligations, that would compel companies to weaken or infringe their users' privacy. In this regard, online platforms and services providers should be encouraged, rather than discouraged or prohibited, to implement strong encryption to ensure users' privacy and security. Such protections will also ensure that these platforms and services remain trusted and reliable spaces for exercising freedom of expression, association, peaceful assembly, and other rights.

**18 In your view, what information should online platforms make available in relation to their policy and measures taken with regard to content and goods offered by their users? Please elaborate, with regard to the identification of illegal content and goods, removal, blocking or demotion of content or goods offered, complaints mechanisms and reinstatement, the format and frequency of such information, and who can access the information.**

*5,000 character(s) maximum*



Companies have already taken a range of actions to improve the transparency of their practices. The EU should conduct its own study on the subject, and carefully evaluate the existing analyses.

The DSA should make clear what information must be made public by which types of online platforms, recognizing that different information may be more or less relevant to different services. In addition, the timing, format, and frequency of such reports should be structured so as to ensure that they do not act as competitive barriers for smaller companies.

The DSA should avoid setting "compliance" targets or benchmarks related to content/activity sanctions and recognize that such targets, as well as overly rigid transparency obligations, may unintentionally encourage online platforms to change their rules and procedures in ways that appear to demonstrate "compliance," while actually undermining policy goals and user rights.

Notwithstanding these precautions, covered online platforms could be required to: (i) make clear what processes and tools they rely on to identify illegal content/activity; (ii) make their terms of service and procedures for identifying possibly infringing content/activity, as well as the reasons for changes thereto, clear and publicly available; and (iii) periodically report on the number of notices of illegal and otherwise improper content/activity received, as well as who those comes from, what law or term they were alleged to violate, and what action, if any, was taken.

The DSA should also ensure that online platforms of a certain size provide adequate remedial mechanisms for users whose content is restricted and non-users who may be impacted by content/behavior on their platforms. Periodic audits could ensure that particular users or vulnerable groups, who may fail to take advantage of the due process, are not being unduly impacted.

**19 What type of information should be shared with users and/or competent authorities and other third parties such as trusted researchers with regard to the use of automated systems used by online platforms to detect, remove and/or block illegal content, goods, or user accounts?**

*5,000 character(s) maximum*

With respect to automated tools for detecting and evaluating illegal content/activity, technical details such as source code may be difficult to understand and even where it is understandable, it may not be relevant to any assessment of the impacts that automated systems may have. This information can also be commercially sensitive. Instead, the DSA could require covered online platforms to make clear: 1) what types of tools they are using and for what purposes; 2) what automated decision making approach each tool uses (natural language processing, hashing, etc.); 3) the division and sequencing of human oversight and automated decision making; 4) accuracy/error rates of removal - not only numbers, but also how accuracy is defined; 5) how often algorithmic tools are updated to avoid outdated material; 6) what types and sources of training data are used; and 7) the extent to which such systems are tested for bias and the results of such tests.

20 In your view, what measures are necessary with regard to algorithmic recommender systems used by online platforms?

*5,000 character(s) maximum*

Algorithms and algorithmic systems have been shown to have negative impacts for human rights and user rights in some instances. But they also play important and useful roles in helping to curate the vast amount of content that is available on many online platforms. Given this, and the fact that algorithms are often unable to effectively distinguish illegal content, efforts to make online platforms liable for content that their algorithms recommend or amplify could have unintended impacts. Notwithstanding this concern, platforms can and should be more transparent about how their algorithmic recommender systems function. In addition, regulators should be able to require changes to such systems, in certain limited circumstances where systematic, pernicious impacts of such systems are documented. Users should be able to determine what type of information and criteria are used to filter and rank the information they are presented, including advertising. Platforms should provide users with this information, in a clear, easily accessible, and reliable format. In addition, the DSA could ensure that users have clear and accessible mechanisms to control not only the collection and use of their personal data, but also the criteria by which information is filtered and prioritized to them. In other words, the DSA could require that certain large online services provide users with a choice of whether and how information is presented to them, including choices to enable/disable recommendations.

Furthermore, algorithmic impact assessments can help ensure the design of online platforms' algorithms are rights-respecting and non-discriminatory. If the relevant regulatory agency(ies) are not agile enough or do not possess the interdisciplinary expertise to regularly assess such algorithms, they could consider cooperating with relevant experts from civil society, academia, computer science, and other relevant fields to design and execute such impact assessments.

21 In your view, is there a need for enhanced data sharing between online platforms and authorities, within the boundaries set by the General Data Protection Regulation? Please select the appropriate situations, in your view:

- For supervisory purposes concerning professional users of the platform - e.g. in the context of platform intermediated services such as accommodation or ride-hailing services, for the purpose of labour inspection, for the purpose of collecting tax or social security contributions
- For supervisory purposes of the platforms' own obligations – e.g. with regard to content moderation obligations, transparency requirements, actions taken in electoral contexts and against inauthentic behaviour and foreign interference
- Specific request of law enforcement authority or the judiciary
- On a voluntary and/or contractual basis in the public interest or for other purposes

22 Please explain. What would be the benefits? What would be concerns for companies, consumers or other third parties?

*5,000 character(s) maximum*

Where appropriate protections for user privacy, data protection, and accountability exist, enhanced information sharing could allow for deeper trust and understanding between online platforms and relevant public authorities. However, such bilateral information sharing arrangements raise the potential for undue influence in both directions and should be limited only to scenarios where there are legitimate grounds to restrict additional transparency (i.e., by including trusted researchers, civil society, and/or the public). In addition, the DSA should not be seen as the appropriate instrument for facilitating/requiring access by public authorities to online platform data of all sorts. In particular, where public authorities have made specific demands to online platforms, law enforcement or judicial authorities should not be given additional access to information, as such access - even where well intentioned - could result in undue pressure on online platforms and damage public trust more broadly. More broadly, the proposed e-Evidence framework is specifically designed to address such access. For more on how and when multistakeholder, co-regulatory approaches to information sharing and assessment, please see also our response to Questions 3 and 4 in the section on "Governance and Enforcement" below.

**23 What types of sanctions would be effective, dissuasive and proportionate for online platforms which systematically fail to comply with their obligations (See also the last module of the consultation)?**

*5,000 character(s) maximum*

Sanctions for systematic non-compliance should be clear, specific, and predictable. The level of the sanction should also be proportionate to the severity of the non-compliance (i.e. a one-time offender vs. multiple). In general, significant sanctions should be a measure of last resort. To ensure effective notice, the DSA should require that notices of alleged non-compliance are provided before any sanctions are levied, elucidating the reasons why the online platform is suspected to have systematically failed to comply with their obligations and providing a reasonable opportunity for the platform to respond. If sanctions are levied, platforms must also be allowed to appeal them before an independent adjudicator.

In order to ensure effectiveness and remain consistent with international human rights principles, the DSA should avoid imposing specific, tight time periods for taking action in response to notifications, rigid compliance targets, or obligations to adjudicate under law and/or report allegedly illegal content to authorities (where online platforms discover content that they believe may be illegal, they should nevertheless be encouraged to report it).

**24 Are there other points you would like to raise?**

*3,000 character(s) maximum*

## **II. Reviewing the liability regime of digital services acting as intermediaries?**

The liability of online intermediaries is a particularly important area of internet law in Europe and worldwide. The E-Commerce Directive harmonises the liability exemptions applicable to online intermediaries in the single market, with specific provisions for different services according to their role: from Internet access providers

and messaging services to hosting service providers.

The previous section of the consultation explored obligations and responsibilities which online platforms and other services can be expected to take – i.e. processes they should put in place to address illegal activities which might be conducted by users abusing their service. In this section, the focus is on the legal architecture for the liability regime for service providers when it comes to illegal activities conducted by their users. The Commission seeks informed views on how the current liability exemption regime is working and the areas where an update might be necessary.

2 The liability regime for online intermediaries is primarily established in the E-Commerce Directive, which distinguishes between different types of services: so called ‘mere conduits’, ‘caching services’, and ‘hosting services’.

In your understanding, are these categories sufficiently clear and complete for characterising and regulating today’s digital intermediary services? Please explain.

*5,000 character(s) maximum*

It can be important and useful to distinguish among different types of service providers. Because the three categories established twenty years ago in the E-Commerce Directive (“ECD”) did not anticipate certain services and business models, it has created different degrees of clarity and predictability for different types of intermediaries. For instance, the “mere conduits” and “caching services” categories have been relatively well understood to cover technical services, which has helped to ensure continued innovation and deployment of such services. At the same time, the range of different business models and services that fall under the “hosting services” category has expanded significantly, such that cloud infrastructure and business-to-business services, which generally present lower risk of, visibility into, and control over illegal content are grouped together with social media services. The DSA presents an opportunity to modernize and update this framework to make it clear to all types of intermediaries when they may bear liability for third-party content. In doing so, the DSA should be guided by the principles of necessity and proportionality, as well as a focus on which services present the highest risk of and are best positioned to address illegal content. It can also attempt to future-proof itself by anticipating, to the extent possible, the evolving nature of the information and communication technology (ICT) ecosystem and building in processes for periodic review and reauthorization.

For hosting services, the liability exemption for third parties’ content or activities is conditioned by a knowledge standard (i.e. when they get ‘actual knowledge’ of the illegal activities, they must ‘act expeditiously’ to remove it, otherwise they could be found liable).

3 Are there aspects that require further legal clarification?

*5,000 character(s) maximum*

States should not make intermediaries the ultimate arbiters of illegal speech, as they do not have the necessary legitimacy, authority, or the expertise for such a role. The CJEU's jurisprudence on civil liability for hosting providers has hinged on identifying when an intermediary has "awareness" (also known as "constructive knowledge") of illegal activity or information on its platform. Unfortunately, such an approach plays into the hands of foreign interference campaigns, troll armies, and other malicious actors seeking to manipulate online platforms into silencing particular voices and perspectives. To ensure that freedom of expression is protected online in the EU, the DSA should clarify that the "actual knowledge" standard applies to both criminal and civil liability and that such knowledge can only be established pursuant to an order from an independent adjudicator duly authorized under the law. This will help online platforms to focus and strengthen the transparency, consistency, and accountability of their content moderation efforts.

**4 Does the current legal framework dis-incentivize service providers to take proactive measures against illegal activities? If yes, please provide your view on how disincentives could be corrected.**

*5,000 character(s) maximum*

In a word, yes. The ECD and interpretations of it by the CJEU have made "activeness vs. passiveness" the primary characteristic for distinguishing which hosting intermediaries may face liability for third-party content and when. However, as service providers modify their business models and technologies, this distinction could benefit from further clarification.

The DSA should provide clarity and predictability to all forms of service providers as to what characteristics and/or actions may open them up to liability. In particular, the DSA should include a clear and broad "Good Samaritan" provision to make it clear that proactive steps taken by service providers to identify and address illegal content will not lead to a loss of safe harbor protections. To provide effective protection of fundamental rights and ensure that such proactive measures do not unduly restrict freedom of expression or privacy, the DSA should also include provisions making clear what due process, non-discrimination, transparency, and remedy procedures are expected from covered service providers who actively seek to moderate content.

**5 Do you think that the concept characterising intermediary service providers as playing a role of a 'mere technical, automatic and passive nature' in the transmission of information (recital 42 of the E-Commerce Directive (<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031>)) is sufficiently clear and still valid? Please explain.**

*5,000 character(s) maximum*

Recent CJEU jurisprudence has made it clear that the meaning of recital 42 of the ECD is not sufficiently clear, especially as it regards hosting providers. As noted above, the distinction between 'active' and 'passive' hosting services could benefit from further clarification. Traditional hosting services that have a completely neutral role are small in number. The DSA can create more legal certainty and remove this ambiguity by including all services under the safe harbor and making it clear that they will only be liable if they have 'actual knowledge' of illegal content/activity in the form of an order from a court or another authorized, independent adjudicator.

6 The E-commerce Directive also prohibits Member States from imposing on intermediary service providers general monitoring obligations or obligations to seek facts or circumstances of illegal activities conducted on their service by their users.

In your view, is this approach, balancing risks to different rights and policy objectives, still appropriate today? Is there further clarity needed as to the parameters for 'general monitoring obligations'? Please explain.

*5,000 character(s) maximum*

It is critical to maintain the prohibition on general monitoring obligations. For one, intermediaries do not have the capacity or resources to proactively monitor the diverse amount of content being uploaded by users without jeopardizing fundamental rights. Fearing hefty fines or other sanctions, intermediaries will lean towards proactively over-removing or otherwise limiting any content that could be considered unlawful, but may in fact be lawful or even legally protected, thereby restricting free expression.

In addition, such obligations are likely to force large service providers who handle a high volume of content to rely more on machine learning-enabled tools. Such tools remain too ineffective to be deployed without extensive human oversight and are unlikely to properly assess the legality of content whose interpretation requires cultural, social, and historical context. High Courts in Argentina and India have rejected general monitoring obligations, and civil rights groups continue to raise objections on international law and fundamental rights grounds. General monitoring obligations effectively privatize free expression decisions, and make the process even more opaque to users, academics, policymakers, lawmakers, and other key stakeholders who should be a part of the solution.

7 Do you see any other points where an upgrade may be needed for the liability regime of digital services acting as intermediaries?

*5,000 character(s) maximum*

### III. What issues derive from the gatekeeper power of digital platforms?

There is wide consensus concerning the benefits for consumers and innovation, and a wide-range of efficiencies, brought about by online platforms in the European Union's Single Market. Online platforms facilitate cross-border trading within and outside the EU and open entirely new business opportunities to a variety of European businesses and traders by facilitating their expansion and access to new markets. At the same time, regulators and experts around the world consider that large online platforms are able to control increasingly important online platform ecosystems in the digital economy. Such large online platforms connect many businesses and consumers. In turn, this enables them to leverage their advantages – economies of scale, network effects and important data assets- in one area of their activity to improve or develop new services in adjacent areas. The concentration of economic power in then platform economy creates a small number of 'winner-takes it all/most' online platforms. The winner online platforms can also readily take over (potential) competitors and it is very difficult for an existing competitor or potential new entrant to overcome the winner's competitive edge.

The Commission announced ([https://ec.europa.eu/info/publications/communication-shaping-europes-digital-future\\_en](https://ec.europa.eu/info/publications/communication-shaping-europes-digital-future_en)) that it 'will further explore, in the context of the Digital Services Act package, ex ante rules to ensure that markets characterised by large platforms with significant network effects acting as gatekeepers, remain

fair and contestable for innovators, businesses, and new market entrants’.

This module of the consultation seeks informed views from all stakeholders on this framing, on the scope, the specific perceived problems, and the implications, definition and parameters for addressing possible issues deriving from the economic power of large, gatekeeper platforms.

The Communication ‘Shaping Europe’s Digital Future’ ([https://ec.europa.eu/info/publications/communication-shaping-europes-digital-future\\_en](https://ec.europa.eu/info/publications/communication-shaping-europes-digital-future_en)) also flagged that ‘competition policy alone cannot address all the systemic problems that may arise in the platform economy’. Stakeholders are invited to provide their views on potential new competition instruments through a separate, dedicated open public consultation that will be launched soon.

In parallel, the Commission is also engaged in a process of reviewing EU competition rules and ensuring they are fit for the modern economy and the digital age. As part of that process, the Commission has launched a consultation on the proposal for a New Competition Tool aimed at addressing the gaps identified in enforcing competition rules. The initiative intends to address as specific objectives the structural competition problems that prevent markets from functioning properly and that can tilt the level playing field in favour of only a few market players. This could cover certain digital or digitally-enabled markets, as identified in the report by the Special Advisers and other recent reports on the role of competition policy, and/or other sectors. As such, the work on a proposed new competition tool and the initiative at stake complement each other. The work on the two impact assessments will be conducted in parallel in order to ensure a coherent outcome. In this context, the Commission will take into consideration the feedback received from both consultations. We would therefore invite you, in preparing your responses to the questions below, to also consider your response to the parallel consultation on a new competition tool ([https://ec.europa.eu/eusurvey/runner/New\\_Competition\\_Tool](https://ec.europa.eu/eusurvey/runner/New_Competition_Tool)).

1 To what extent do you agree with the following statements?

	Fully agree	Some what agree	Neither agree not disagree	Somewhat disagree	Fully disagree	I don't know/ No reply
Consumers have sufficient choices and alternatives to the offerings from online platforms.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It is easy for consumers to switch between services provided by online platform companies and use same or similar services provider by other online platform companies (“multi-home”).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It is easy for individuals to port their data in a useful manner to alternative service providers outside of an online platform.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
There is sufficient level of interoperability between services of different online platform companies.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>




There is an asymmetry of information between the knowledge of online platforms about consumers, which enables them to target them with commercial offers, and the knowledge of consumers about market conditions.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It is easy for innovative SME online platforms to expand or enter the market.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Traditional businesses are increasingly dependent on a limited number of very large online platforms.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
There are imbalances in the bargaining power between these online platforms and their business users.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Businesses and consumers interacting with these online platforms are often asked to accept unfavourable conditions and clauses in the terms of use/contract with the online platforms.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Certain large online platform companies create barriers to entry and expansion in the Single Market (gatekeepers).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Large online platforms often leverage their assets from their primary activities (customer base, data, technological solutions, skills, financial capital) to expand into other activities.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When large online platform companies expand into such new activities, this often poses a risk of reducing innovation and deterring competition from smaller innovative market operators.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## **Main features of gatekeeper online platform companies and the main criteria for assessing their economic power**

1 Which characteristics are relevant in determining the gatekeeper role of large online platform companies?  
Please rate each criterion identified below from 1 (not relevant) to 5 (very relevant):

Large user base	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Wide geographic coverage in the EU	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
They capture a large share of total revenue of the market you are active/of a sector	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Impact on a certain sector	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
They build on and exploit strong network effects	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
They leverage their assets for entering new areas of activity	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
They raise barriers to entry for competitors	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
They accumulate valuable and diverse data and information	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>



There are very few, if any, alternative services available on the market	
Lock-in of users/consumers	
Other	

2 If you replied "other", please list

*3,000 character(s) maximum*

3 Please explain your answer. How could different criteria be combined to accurately identify large online platform companies with gatekeeper role?

*3,000 character(s) maximum*

4 Do you believe that the integration of any or all of the following activities within a single company can strengthen the gatekeeper role of large online platform companies ('conglomerate effect')? Please select the activities you consider to strengthen the gatekeeper role:

- online intermediation services (i.e. consumer-facing online platforms such as e-commerce marketplaces, social media, mobile app stores, etc., as per Regulation (EU) 2019/1150 (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R1150>) - see glossary)
- search engines
- operating systems for smart devices
- consumer reviews on large online platforms
- network and/or data infrastructure/cloud services
- digital identity services
- payment services (or other financial services)
- physical logistics such as product fulfilment services
- data management platforms
- online advertising intermediation services
- other. Please specify in the text box below.

5 Other - please list

*1,000 character(s) maximum*

## **Emerging issues**

***The following questions are targeted particularly at businesses and business users of large online platform companies.***

2 As a business user of large online platforms, do you encounter issues concerning trading conditions on large online platform companies?

- Yes  
 No

3 Please specify which issues you encounter and please explain to what types of platform these are related to (e.g. e-commerce marketplaces, app stores, search engines, operating systems, social networks).

*5,000 character(s) maximum*

4 Have you been affected by unfair contractual terms or unfair practices of very large online platform companies? Please explain your answer in detail, pointing to the effects on your business, your consumers and possibly other stakeholders in the short, medium and long-term?

*5,000 character(s) maximum*

---

***The following questions are targeted particularly at consumers who are users of large online platform companies.***

6 Do you encounter issues concerning commercial terms and conditions when accessing services provided by large online platform companies?

Please specify which issues you encounter and please explain to what types of platform these are related to (e.g. e-commerce marketplaces, app stores, search engines, operating systems, social networks).

*5,000 character(s) maximum*

7 Have you considered any of the practices by large online platform companies as unfair? Please explain.

*3,000 character(s) maximum*

---

***The following questions are open to all respondents.***

9 Are there specific issues and unfair practices you perceive on large online platform companies?

*5,000 character(s) maximum*

10 In your view, what practices related to the use and sharing of data in the platforms' environment are raising particular challenges?

*5,000 character(s) maximum*

11 What impact would the identified unfair practices can have on innovation, competition and consumer choice in the single market?

*3,000 character(s) maximum*

12 Do startups or scaleups depend on large online platform companies to access or expand? Do you observe any trend as regards the level of dependency in the last five years (i.e. increases; remains the same; decreases)? Which difficulties in your view do start-ups or scale-ups face when they depend on large online platform companies to access or expand on the markets?

*3,000 character(s) maximum*

13 Which are possible positive and negative societal (e.g. on freedom of expression, consumer protection, media plurality) and economic (e.g. on market contestability, innovation) effects, if any, of the gatekeeper role that large online platform companies exercise over whole platform ecosystem?

*3,000 character(s) maximum*

14 Which issues specific to the media sector (if any) would, in your view, need to be addressed in light of the gatekeeper role of large online platforms? If available, please provide additional references, data and facts.

*3,000 character(s) maximum*

## **Regulation of large online platform companies acting as gatekeepers**

1 Do you believe that in order to address any negative societal and economic effects of the gatekeeper role that large online platform companies exercise over whole platform ecosystems, there is a need to consider dedicated regulatory rules?

- I fully agree
- I agree to a certain extent
- I disagree to a certain extent
- I disagree
- I don't know

2 Please explain

*3,000 character(s) maximum*

3 Do you believe that such dedicated rules should prohibit certain practices by large online platform companies with gatekeeper role that are considered particularly harmful for users and consumers of these large online platforms?

- Yes
- No
- I don't know

4 Please explain your reply and, if possible, detail the types of prohibitions that should in your view be part of the regulatory toolbox.

*3,000 character(s) maximum*

5 Do you believe that such dedicated rules should include obligations on large online platform companies with gatekeeper role?

- Yes
- No
- I don't know

6 Please explain your reply and, if possible, detail the types of obligations that should in your view be part of the regulatory toolbox.

*3,000 character(s) maximum*

7 If you consider that there is a need for such dedicated rules setting prohibitions and obligations, as those referred to in your replies to questions 3 and 5 above, do you think there is a need for a specific regulatory authority to enforce these rules?

- Yes
- No
- I don't know

8 Please explain your reply.

*3,000 character(s) maximum*

9 Do you believe that such dedicated rules should enable regulatory intervention against specific large online platform companies, when necessary, with a case by case adapted remedies?

- Yes
- No
- I don't know

10 If yes, please explain your reply and, if possible, detail the types of case by case remedies.

*3,000 character(s) maximum*

11 If you consider that there is a need for such dedicated rules, as referred to in question 9 above, do you think there is a need for a specific regulatory authority to enforce these rules?

- Yes
- No

12 Please explain your reply

*3,000 character(s) maximum*

13 If you consider that there is a need for a specific regulatory authority to enforce dedicated rules referred to questions 3, 5 and 9 respectively, would in your view these rules need to be enforced by the same regulatory authority or could they be enforced by different regulatory authorities? Please explain your reply.

*3,000 character(s) maximum*

14 At what level should the regulatory oversight of platforms be organised?

- At national level
- At EU level
- Both at EU and national level.
- I don't know

15 If you consider such dedicated rules necessary, what should in your view be the relationship of such rules with the existing sector specific rules and/or any future sector specific rules?

*3,000 character(s) maximum*

16 Should such rules have an objective to tackle both negative societal and negative economic effects deriving from the gatekeeper role of these very large online platforms? Please explain your reply.

*3,000 character(s) maximum*

17 Specifically, what could be effective measures related to data held by very large online platform companies with a gatekeeper role beyond those laid down in the General Data Protection Regulation in order to promote competition and innovation as well as a high standard of personal data protection and consumer welfare?

*3,000 character(s) maximum*

18 What could be effective measures concerning large online platform companies with a gatekeeper role in order to promote media pluralism, while respecting the subsidiarity principle?

*3,000 character(s) maximum*

19 Which, if any, of the following characteristics are relevant when considering the requirements for a potential regulatory authority overseeing the large online platform companies with the gatekeeper role:

- Institutional cooperation with other authorities addressing related sectors – e.g. competition authorities, data protection authorities, financial services authorities, consumer protection authorities, cyber security, etc.
- Pan-EU scope
- Swift and effective cross-border cooperation and assistance across Member States
- Capacity building within Member States
- High level of technical capabilities including data processing, auditing capacities
- Cooperation with extra-EU jurisdictions
- Other

21 Please explain if these characteristics would need to be different depending on the type of ex ante rules (see questions 3, 5, 9 above) that the regulatory authority would be enforcing?

*3,000 character(s) maximum*

22 Which, if any, of the following requirements and tools could facilitate regulatory oversight over very large online platform companies (multiple answers possible):

- Reporting obligation on gatekeeping platforms to send a notification to a public authority announcing its intention to expand activities
- Monitoring powers for the public authority (such as regular reporting)
- Investigative powers for the public authority
- Other

24 Please explain if these requirements would need to be different depending on the type of ex ante rules (see questions 3, 5, 9 above) that the regulatory authority would be enforcing?

3,000 character(s) maximum

25 Taking into consideration the parallel consultation on a proposal for a New Competition Tool ([https://ec.europa.eu/eusurvey/runner/New\\_Competition\\_Tool](https://ec.europa.eu/eusurvey/runner/New_Competition_Tool)) focusing on addressing structural competition problems that prevent markets from functioning properly and tilt the level playing field in favour of only a few market players. Please rate the suitability of each option below to address market issues arising in online platforms ecosystems. Please rate the policy options below from 1 (not effective) to 5 (most effective).

	1 (not effective)	2 (somewhat effective)	3 (sufficiently effective)	4 (very effective)	5 (most effective)	Not applicable/No relevant experience or knowledge
1. Current competition rules are enough to address issues raised in digital markets	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. There is a need for an additional regulatory framework imposing obligations and prohibitions that are generally applicable to all large online platforms with gatekeeper power	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. There is a need for an additional regulatory framework allowing for the possibility to impose tailored remedies on individual large online platforms with gatekeeper power, on a case-by-case basis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. There is a need for a New Competition Tool allowing to address structural risks and lack of competition in (digital) markets on a case-by-case basis.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5. There is a need for combination of two or more of the options 2 to 4.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

26 Please explain which of the options, or combination of these, would be, in your view, suitable and sufficient to address the market issues arising in the online platforms ecosystems.

3,000 character(s) maximum

27 Are there other points you would like to raise?

3,000 character(s) maximum

## IV. Other emerging issues and opportunities, including online advertising and smart contracts

---

Online advertising has substantially evolved over the recent years and represents a major revenue source for many digital services, as well as other businesses present online, and opens unprecedented opportunities for content creators, publishers, etc. To a large extent, maximising revenue streams and optimising online advertising are major business incentives for the business users of the online platforms and for shaping the data policy of the platforms. At the same time, revenues from online advertising as well as increased visibility and audience reach are also a major incentive for potentially harmful intentions, e.g. in online disinformation campaigns.

Another emerging issue is linked to the conclusion of ‘smart contracts’ which represent an important innovation for digital and other services, but face some legal uncertainties.

This section of the open public consultation seeks to collect data, information on current practices, and informed views on potential issues emerging in the area of online advertising and smart contracts.

Respondents are invited to reflect on other areas where further measures may be needed to facilitate innovation in the single market. This module does not address privacy and data protection concerns; all aspects related to data sharing and data collection are to be afforded the highest standard of personal data protection.

### **Online advertising**

1 When you see an online ad, is it clear to you who has placed it online?

- Yes, always
- Sometimes: but I can find the information when this is not immediately clear
- Sometimes: but I cannot always find this information
- I don't know
- No

2 As a publisher online (e.g. owner of a website where ads are displayed), what types of advertising systems do you use for covering your advertising space? What is their relative importance?

	% of ad space	% of ad revenue
Intermediated programmatic advertising through real-time bidding		
Private marketplace auctions		

Programmatic advertising with guaranteed impressions (non-auction based)		
Behavioural advertising (micro-targeting)		
Contextual advertising		
Other		


3 What information is publicly available about ads displayed on an online platform that you use?

3,000 character(s) maximum

4 As a publisher, what type of information do you have about the advertisement placed next to your content/on your website?

3,000 character(s) maximum

5 To what extent do you find the quality and reliability of this information satisfactory for your purposes?

Please rate your level of satisfaction	
--	---


6 As an advertiser or an agency acting on behalf of the advertiser (if applicable), what types of programmatic advertising do you use to place your ads? What is their relative importance in your ad inventory?

	% of ad inventory	% of ad expenditure
Intermediated programmatic advertising through real-time bidding		
Private marketplace auctions		
Programmatic advertising with guaranteed impressions (non-auction based)		
Behavioural advertising (micro-targeting)		
Contextual advertising		
Other		

7 As an advertiser or an agency acting on behalf of the advertiser (if applicable), what type of information do you have about the ads placed online on your behalf?

3,000 character(s) maximum

8 To what extent do you find the quality and reliability of this information satisfactory for your purposes?

Please rate your level of satisfaction	
--	---

**The following questions are targeted specifically at online platforms.**

10 As an online platform, what options do your users have with regards to the advertisements they are served and the grounds on which the ads are being served to them? Can users access your service through other



conditions than viewing advertisements? Please explain.

*3,000 character(s) maximum*

11 Do you publish or share with researchers, authorities or other third parties detailed data on ads published, their sponsors and viewership rates? Please explain.

*3,000 character(s) maximum*

12 What systems do you have in place for detecting illicit offerings in the ads you intermediate?

*3,000 character(s) maximum*

---

***The following questions are open to all respondents.***

14 Based on your experience, what actions and good practices can tackle the placement of ads next to illegal content or goods, and/or on websites that disseminate such illegal content or goods, and to remove such illegal content or goods when detected?

*3,000 character(s) maximum*

15 From your perspective, what measures would lead to meaningful transparency in the ad placement process?

*3,000 character(s) maximum*

16 What information about online ads should be made publicly available?

*3,000 character(s) maximum*

17 Based on your expertise, which effective and proportionate auditing systems could bring meaningful accountability in the ad placement system?

*3,000 character(s) maximum*

18 What is, from your perspective, a functional definition of 'political advertising'? Are you aware of any specific obligations attached to 'political advertising' at national level ?

*3,000 character(s) maximum*

19 What information disclosure would meaningfully inform consumers in relation to political advertising? Are there other transparency standards and actions needed, in your opinion, for an accountable use of political advertising and political messaging?

*3,000 character(s) maximum*

20 What impact would have, in your view, enhanced transparency and accountability in the online advertising value chain, on the gatekeeper power of major online platforms and other potential consequences such as media pluralism?

*3,000 character(s) maximum*

21 Are there other emerging issues in the space of online advertising you would like to flag?

*3,000 character(s) maximum*

## **Smart contracts**

1 Is there sufficient legal clarity in the EU for the provision and use of “smart contracts” – e.g. with regard to validity, applicable law and jurisdiction?

Please rate from 1 (lack of clarity) to 5 (sufficient clarity)



2 Please explain the difficulties you perceive.

*3,000 character(s) maximum*

3 In which of the following areas do you find necessary further regulatory clarity?

- Mutual recognition of the validity of smart contracts in the EU as concluded in accordance with the national law
- Minimum standards for the validity of “smart contracts” in the EU
- Measures to ensure that legal obligations and rights flowing from a smart contract and the functioning of the smart contract are clear and unambiguous, in particular for consumers
- Allowing interruption of smart contracts
- Clarity on liability for damage caused in the operation of a smart contract
- Further clarity for payment and currency-related smart contracts.

4 Please explain.

*3,000 character(s) maximum*

5 Are there other points you would like to raise?

*3,000 character(s) maximum*

## V. How to address challenges around the situation of self-employed individuals offering services through online platforms?

---

Individuals providing services through platforms may have different legal status (workers or self-employed). This section aims at gathering first information and views on the situation of self-employed individuals offering services through platforms (such as ride-hailing, food delivery, domestic work, design work, micro-tasks etc.). Furthermore, it seeks to gather first views on whether any detected problems are specific to the platform economy and what would be the perceived obstacles to the improvement of the situation of individuals providing services through platforms. This consultation is not intended to address the criteria by which persons providing services on such platforms are deemed to have one or the other legal status. The issues explored here do not refer to the selling of goods (e.g. online marketplaces) or the sharing of assets (e.g. sub-renting houses) through platforms.

***The following questions are targeting self-employed individuals offering services through online platforms.***

### Relationship with the platform and the final customer

1 What type of service do you offer through platforms?

- Food-delivery
- Ride-hailing
- Online translations, design, software development or micro-tasks
- On-demand cleaning, plumbing or DIY services
- Other, please specify

2 Please explain.

3 Which requirements were you asked to fulfill in order to be accepted by the platform(s) you offer services through, if any?

4 Do you have a contractual relationship with the final customer?

- Yes
- No

5 Do you receive any guidelines or directions by the platform on how to offer your services?

- Yes
- No

7 Under what conditions can you stop using the platform to provide your services, or can the platform ask you to stop doing so?

8 What is your role in setting the price paid by the customer and how is your remuneration established for the services you provide through the platform(s)?

9 What are the risks and responsibilities you bear in case of non-performance of the service or unsatisfactory performance of the service?

### **Situation of self-employed individuals providing services through platforms**

10 What are the main advantages for you when providing services through platforms?

*3,000 character(s) maximum*

11 What are the main issues or challenges you are facing when providing services through platforms? Is the platform taking any measures to improve these?

*3,000 character(s) maximum*

12 Do you ever have problems getting paid for your service? Does/do the platform have any measures to support you in such situations?

*3,000 character(s) maximum*

13 Do you consider yourself in a vulnerable or dependent situation in your work (economically or otherwise), and if yes, why?

14 Can you collectively negotiate vis-à-vis the platform(s) your remuneration or other contractual conditions?

- Yes  
 No

15 Please explain.

---

***The following questions are targeting online platforms.***

### **Role of platforms**

17 What is the role of your platform in the provision of the service and the conclusion of the contract with the customer?

18 What are the risks and responsibilities borne by your platform for the non-performance of the service or unsatisfactory provision of the service?

19 What happens when the service is not paid for by the customer/client?

20 Does your platform own any of the assets used by the individual offering the services?

- Yes  
 No

22 Out of the total number of service providers offering services through your platform, what is the percentage of self-employed individuals?

- Over 75%  
 Between 50% and 75%  
 Between 25% and 50%  
 Less than 25%

## Rights and obligations

23 What is the contractual relationship between the platform and individuals offering services through it?

*3,000 character(s) maximum*

24 Who sets the price paid by the customer for the service offered?

- The platform  
 The individual offering services through the platform  
 Others, please specify

25 Please explain.

*3,000 character(s) maximum*

26 How is the price paid by the customer shared between the platform and the individual offering the services through the platform?

*3,000 character(s) maximum*

27 On average, how many hours per week do individuals spend offering services through your platform?

*3,000 character(s) maximum*

28 Do you have measures in place to enable individuals providing services through your platform to contact each other and organise themselves collectively?

- Yes
- No

29 Please describe the means through which the individuals who provide services on your platform contact each other.

3,000 character(s) maximum

30 What measures do you have in place for ensuring that individuals offering services through your platform work legally - e.g. comply with applicable rules on minimum working age, hold a work permit, where applicable - if any?

(If you replied to this question in your answers in the first module of the consultation, there is no need to repeat your answer here.)

3,000 character(s) maximum

***The following questions are open to all respondents***

**Situation of self-employed individuals providing services through platforms**

32 Are there areas in the situation of individuals providing services through platforms which would need further improvements? Please rate the following issues from 1 (no improvements needed) to 5 (substantial issues need to be addressed).

	1 (no improvements needed)	2	3	4	5 (substantial improvements needed)	I don't know / No answer
Earnings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Flexibility of choosing when and /or where to provide services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transparency on remuneration	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Measures to tackle non-payment of remuneration	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transparency in online ratings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ensuring that individuals providing services through platforms can contact each other and organise themselves for collective purposes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Tackling the issue of work carried out by individuals lacking legal permits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Prevention of discrimination of individuals providing services through platforms, for instance based on gender, racial or ethnic origin	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Allocation of liability in case of damage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other, please specify	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

33 Please explain the issues that you encounter or perceive.

3,000 character(s) maximum

34 Do you think individuals providing services in the 'offline/traditional' economy face similar issues as individuals offering services through platforms?

- Yes
- No
- I don't know

35 Please explain and provide examples.

3,000 character(s) maximum

36 In your view, what are the obstacles for improving the situation of individuals providing services

1. through platforms?
2. in the offline/traditional economy?

3,000 character(s) maximum

37 To what extent could the possibility to negotiate collectively help improve the situation of individuals offering services:

through online platforms?	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
in the offline/traditional economy?	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>

38 Which are the areas you would consider most important for you to enable such collective negotiations?

3,000 character(s) maximum

39 In this regard, do you see any obstacles to such negotiations?

3,000 character(s) maximum

40 Are there other points you would like to raise?

3,000 character(s) maximum



## VI. What governance for reinforcing the Single Market for digital services?

The EU's Single Market offers a rich potential for digital services to scale up, including for innovative European companies. Today there is a certain degree of legal fragmentation in the Single Market . One of the main objectives for the Digital Services Act will be to improve opportunities for innovation and 'deepen the Single Market for Digital Services ([https://ec.europa.eu/info/publications/communication-shaping-europes-digital-future\\_en](https://ec.europa.eu/info/publications/communication-shaping-europes-digital-future_en))'.

This section of the consultation seeks to collect evidence and views on the current state of the single market and steps for further improvements for a competitive and vibrant Single market for digital services. This module also inquires about the relative impact of the COVID-19 crisis on digital services in the Union. It then focuses on the appropriate governance and oversight over digital services across the EU and means to enhance the cooperation across authorities for an effective supervision of services and for the equal protection of all citizens across the single market. It also inquires about specific cooperation arrangements such as in the case of consumer protection authorities across the Single Market, or the regulatory oversight and cooperation mechanisms among media regulators. This section is not intended to focus on the enforcement of EU data protection rules (GDPR).

### **Main issues**

1 How important are - in your daily life or for your professional transactions - digital services such as accessing websites, social networks, downloading apps, reading news online, shopping online, selling products online?

Overall	
Those offered from outside of your Member State of establishment	

### ***The following questions are targeted at digital service providers***

3 Approximately, what share of your EU turnover is generated by the provision of your service outside of your main country of establishment in the EU?

- Less than 10%
- Between 10% and 50%
- Over 50%
- I cannot compute this information

4 To what extent are the following obligations a burden for your company in providing its digital services, when expanding to one or more EU Member State(s)? Please rate the following obligations from 1 (not at all burdensome) to 5 (very burdensome).



	1 (not at all burdensome)	2	3 (neutral)	4	5 (very burdensome)	I don't know / No answer
Different processes and obligations imposed by Member States for notifying, detecting and removing illegal content/goods/services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Requirements to have a legal representative or an establishment in more than one Member State	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Different procedures and points of contact for obligations to cooperate with authorities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other types of legal requirements. Please specify below	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

6 Have your services been subject to enforcement measures by an EU Member State other than your country of establishment?

- Yes
- No
- I don't know

8 Were you requested to comply with any 'prior authorisation' or equivalent requirement for providing your digital service in an EU Member State?

- Yes
- No
- I don't know

10 Are there other issues you would consider necessary to facilitate the provision of cross-border digital services in the European Union?

*3,000 character(s) maximum*

11 What has been the impact of COVID-19 outbreak and crisis management measures on your business' turnover

- Significant reduction of turnover
- Limited reduction of turnover
- No significant change
- Modest increase in turnover
- Significant increase of turnover
- Other

13 Do you consider that deepening of the Single Market for digital services could help the economic recovery of your business?

- Yes  
 No  
 I don't know

14 Please explain

3,000 character(s) maximum

---

***The following questions are targeted at all respondents.***

---

## **Governance of digital services and aspects of enforcement**

The 'country of origin' principle is the cornerstone of the Single Market for digital services. It ensures that digital innovators, including start-ups and SMEs, have a single set of rules to follow (that of their home country), rather than 27 different rules.

This is an important precondition for services to be able to scale up quickly and offer their services across borders. In the aftermath of the COVID-19 outbreak and effective recovery strategy, more than ever, a strong Single Market is needed to boost the European economy and to restart economic activity in the EU.

At the same time, enforcement of rules is key; the protection of all EU citizens regardless of their place of residence, will be in the centre of the Digital Services Act.

The current system of cooperation between Member States foresees that the Member State where a provider of a digital service is established has the duty to supervise the services provided and to ensure that all EU citizens are protected. A cooperation mechanism for cross-border cases is established in the E-Commerce Directive.

1 Based on your experience, how would you assess the cooperation in the Single Market between authorities entrusted to supervise digital services?

5,000 character(s) maximum

Single Market cooperation between authorities should be updated to establish a modern system of supervision that fits the current digital services landscape. This supervision and effective enforcement should be coordinated at the EU level, as digital services are offered globally and affect different EU countries across borders. In addition, coordination with competent national authorities is necessary to take into account the offering of different services in different Member States and in order to facilitate enforcement.

2 What governance arrangements would lead to an effective system for supervising and enforcing rules on online platforms in the EU in particular as regards the intermediation of third party goods, services and content (See also Chapter 1 of the consultation)?

Please rate each of the following aspects, on a scale of 1 (not at all important) to 5 (very important).

	1 (not at all important)	2	3 (neutral)	4	5 (very important)	I d o n' t k n o w / N o a n s w e r
Clearly assigned competent national authorities or bodies as established by Member States for supervising the systems put in place by online platforms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cooperation mechanism within Member States across different competent authorities responsible for the systematic supervision of online platforms and sectorial issues (e.g. consumer protection, market surveillance, data protection, media regulators, anti-discrimination agencies, equality bodies, law enforcement authorities etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cooperation mechanism with swift procedures and assistance across national competent authorities across Member States	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Coordination and technical assistance at EU level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
An EU-level authority	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cooperation schemes with third parties such as civil society organisations and academics for specific inquiries and oversight	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Other: please specify in the text box below	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

### 3 Please explain

5,000 character(s) maximum

Clarity, consistency, and predictability are particularly important measures that can ensure that regulatory supervision and enforcement is effective and proportionate. The DSA should ensure that relevant enforcement mechanisms and authorities are clearly established/identified and supported for each of the regulatory requirements that intermediaries are subject to.

In general, the DSA should seek to minimize redundancies and the potential for conflicts between relevant authorities, while maximizing their expertise and effectiveness. Certain activities can only be carried out by public authorities. Some of these, such as providing authoritative guidance for interpretation of the DSA, may be more appropriately supervised and enforced by an EU-level authority. Other responsibilities, such as investigating alleged breaches of the DSA, may benefit from a more federated approach. Other aspects of the DSA can and should involve and leverage the broad expertise, legitimacy, and interest of civil society, academics, and technical experts.

For over a decade, the Global Network Initiative has been working to define and refine an assessment process for reviewing company members' implementation of the GNI's Principles on Freedom of Expression and Privacy and related Implementation Guidelines. Over the course of our work, we have demonstrated how a multistakeholder approach to reviewing sensitive company procedures and activities can maintain confidentiality while providing meaningful insight that facilitates shared learning, collaborative problem solving, and accountability for an increasingly diverse range of ICT companies (including online platforms, telecommunication companies, and equipment vendors). By providing and facilitating a trusted and managed platform for information sharing, overseen by a multistakeholder governance framework, GNI has helped advance freedom of expression and privacy in the ICT sector, focusing specifically on the ways companies respond to government demands and restrictions. The DSA should consider using similar frameworks for multistakeholder information sharing and assessment, which can be particularly useful for achieving transparency and accountability where legitimate data protection, privacy, competition or other concerns may limit the degree to which information can be made public, where a broad range of perspectives and expertise may be necessary to adequately understand the impacts of online platform behavior, and/or where collaboration and coordination among diverse actors is necessary to achieve public policy outcomes.

#### 4 What information should competent authorities make publicly available about their supervisory and enforcement activity?

*3,000 character(s) maximum*

Transparency and accountability mechanisms are just as important for governments, as they are for intermediaries. Competent authorities should make as much information about their supervisory and enforcement activities under the DSA public as possible. The DSA should articulate a default expectation of transparency on the part of competent authorities, clearly setting out limited, legitimate grounds and procedures for keeping such information confidential and ensuring that transparency is achieved as soon as practicable after such conditions have passed.

The DSA should also make it clear that EU and member state authorities are required to regularly publish information about the legal orders and referrals they send to intermediaries, including the number of such notices broken out by the legal basis, underlying content/behavior of concern, and the requesting government agency. Such transparency should extend to civil court orders mandating that intermediaries take certain action with respect to content. The DSA should also ensure that companies are allowed to publish information about such notices, including where appropriate their content. Such transparency is particularly important in the context of Internet Referral Units (IRUs), which are increasingly active at the European and member state levels. IRUs flag content for removal based on a company's terms of service, and not based on local law, raising transparency and accountability concerns and existing transparency reporting and accountability measures for such activities are inadequate.

**5 What capabilities – type of internal expertise, resources etc. - are needed within competent authorities, in order to effectively supervise online platforms?**

*3,000 character(s) maximum*

The range of expertise and resources that will be needed to effectively supervise and enforce the DSA will necessarily depend on the regulation's scope. However, a study by the IMCO Committee suggests that public authorities may not have the sufficient expertise to supervise online platforms, and may need to be complemented by private bodies. As noted above in response to Q3, such external expertise can be incorporated through appropriately designed, co-regulatory mechanisms.

**6 In your view, is there a need to ensure similar supervision of digital services established outside of the EU that provide their services to EU users?**

- Yes, if they intermediate a certain volume of content, goods and services provided in the EU
- Yes, if they have a significant number of users in the EU
- No
- Other
- I don't know

**7 Please explain**

*3,000 character(s) maximum*

As noted in response to question 7 under the safety and responsibility section, the EU should take care to ensure that the DSA does not create unnecessary conflicts of law, or otherwise strain international comity. The most rational and effective way to establish regulatory jurisdiction over digital services is to base it upon the extent to which the underlying activity/ies being regulated have impacts within the EU. While the number of EU-based users of a given service may be relatively easy to determine, it is a poor proxy for the actual impacts or effects of a particular service. For instance, a service with ten-million EU-based users who infrequently use it, will have less impact than a service with half as many very actively engaged users. In addition, certain types of services may have significantly greater impacts than others based on, among other things, their design, their user base, and the extent to which their activities are also regulated by other jurisdictions.

**8 How should the supervision of services established outside of the EU be set up in an efficient and coherent manner, in your view?**

*3,000 character(s) maximum*

Where digital services based outside of the EU clearly meet the impact/affect criteria articulated above in response to Q7, they may be required to create or designate an office and/or point of contact in a EU member state in order to establish appropriate personal jurisdiction.

**9 In your view, what governance structure could ensure that multiple national authorities, in their respective areas of competence, supervise digital services coherently and consistently across borders?**

*3,000 character(s) maximum*

A centralized EU regulatory body could be charged with communication with and coordination of relevant member state authorities in order to achieve coherent and consistent supervision and enforcement of the DSA..

**10 As regards specific areas of competence, such as on consumer protection or product safety, please share your experience related to the cross-border cooperation of the competent authorities in the different Member States.**






*3,000 character(s) maximum*

**11 In the specific field of audiovisual, the Audiovisual Media Services Directive established a regulatory oversight and cooperation mechanism in cross border cases between media regulators, coordinated at EU level within European Regulators' Group for Audiovisual Media Services (ERGA). In your view is this sufficient to ensure that users remain protected against illegal and harmful audiovisual content (for instance if services are offered to users from a different Member State)? Please explain your answer and provide practical examples if you consider the arrangements may not suffice.**

*3,000 character(s) maximum*

**12 Would the current system need to be strengthened? If yes, which additional tasks be useful to ensure a more effective enforcement of audiovisual content rules?**

Please assess from 1 (least beneficial) – 5 (most beneficial). You can assign the same number to the same actions should you consider them as being equally important.

Coordinating the handling of cross-border cases, including jurisdiction matters	
Agreeing on guidance for consistent implementation of rules under the AVMSD	
Ensuring consistency in cross-border application of the rules on the promotion of European works	
Facilitating coordination in the area of disinformation	
Other areas of cooperation	

13 Other areas of cooperation - (please, indicate which ones)

*3,000 character(s) maximum*

14 Are there other points you would like to raise?

*3,000 character(s) maximum*

## Final remarks

---

If you wish to upload a position paper, article, report, or other evidence and data for the attention of the European Commission, please do so.

1 Upload file

2 Other final comments

*3,000 character(s) maximum*

In early October, the Global Network Initiative (GNI) will publish a "Content Regulation Policy Brief" based on our review of over a dozen recent governmental initiatives that claim to address various forms of online harm related to user-generated content – a practice we refer to broadly as "content regulation." We focused on proposals that could shift existing responsibilities and incentives related to user-generated content. Our analysis illustrates the ways that good governance and human rights principles provide time-tested guidance for how laws, regulations, and policy actions can be most appropriately and effectively designed and carried out. Because content regulation is primarily focused on and likely to impact digital communication and content, we use international human rights principles related to freedom of expression and privacy as our primary lens.

These historically validated human rights principles can help lawmakers find creative and appropriate ways to engage stakeholders, design fit-for-purpose regulations, and mitigate unintended consequences. Governments that actively place human rights at the forefront of their deliberations and designs are not only less likely to infringe on their own hallowed commitments, they can also achieve more informed and effective outcomes, balancing public and private responsibilities, designing appropriate incentives, enhancing trust, and fostering innovation.

We look forward to sharing this Policy Brief with European officials and other stakeholders and very much hope that it will be useful as the conversation continues around EU content regulation efforts, including the DSA. GNI looks forward to continuing to participate in those conversations.

## Useful links

Digital Services Act package (<https://ec.europa.eu/digital-single-market/en/digital-services-act-package>)  
(<https://ec.europa.eu/digital-single-market/en/digital-services-act-package>)

---

## Background Documents

(BG) Речник на термините

(CS) Glossář

(DA) Ordliste

(DE) Glossar

(EL) Γλωσσάριο

(EN) Glossary

(ES) Glosario

(ET) Sõnastik

(FI) Sanasto

(FR) Glossaire

(HR) Pojmovnik

(HU) Glosszárium

(IT) Glossario

(LT) Žodynėlis



(LV) Glosārijs

(MT) Glossarju

(NL) Verklarende woordenlijst

(PL) Słowniczek

(PT) Glossário

(RO) Glosar

(SK) Slovník

(SL) Glosar

(SV) Ordlista

---

## Contact

CNECT-consultation-DSA@ec.europa.eu

---