Contribution ID: 0e04f6a1-cd10-415f-b337-d5978faad247
Date: 08/09/2020 08:06:05

Digital Services Act package: open public consultation

Fields marked with * are mandatory.

Introduction

The Commission recently announced 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.

How to respond

Make sure to **save tour 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

○ Bulgarian
○ Croatian
○ Czech
○ Danish
○ Dutch
● English
○ Estonian
○ Finnish

○ French
○ Gaelic
○ German
○ Greek
○ Hungarian
○ Italian
○ Latvian
○ Lithuanian
○ Maltese
○ Polish
○ Portuguese
○ Romanian
○ Slovak
○ Slovenian
○ Spanish
○ Swedish

*2 I am giving my contribution as

○ Academic/research institution
● Business association
○ Company/business organisation
○ Consumer organisation
○ EU citizen
○ Environmental organisation
○ Non-EU citizen
○ Non-governmental organisation (NGO)
○ Public authority
○ Trade union
○ Other

*3 First name

EDiMA

*4 Surname

EDIMA

*5 Email (this won't be published)

info@edima-eu.org

*7 Organisation name

255 character(s) maximum

EDiMA

*8 Organisation size

- ● Micro (1 to 9 employees)
- ○ Small (10 to 49 employees)
- ○ Medium (50 to 249 employees)
- ○ Large (250 or more)

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

11 Would you describe your company as :

- □ a startup?
- □ a scaleup?
- □ a conglomerate offering a wide range of services online?

12 Is your organisation:

- □ an online intermediary
- ☑ an association representing the interests of online intermediaries
- □ a digital service provider, other than an online intermediary
- ☑ an association representing the interests of such digital services
- □ a different type of business than the options above
- □ an association representing the interest of such businesses

□ other

13 What type(s) of services do you provide?

□ Internet access provider
□ Domain name services
□ Messaging service between a finite number of users
□ Cloud computing services
□ E-commerce market place: for sales of goods, travel and accommodation booking, etc.
□ Collaborative economy platform
□ Social networking
□ Video, audio and image sharing
□ File hosting and sharing
□ News and media sharing
□ App distribution
□ Rating and reviews
□ Price comparison
□ Video streaming
□ Online advertising intermediation
□ Blog hosting
□ Other services

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

19 Please select the EU Member States where your organisation is established or currently has a legal representative in:

○ Austria

● Belgium

○ Bulgaria

○ Croatia

○ Cyprus

○ Czechia

○ Denmark

○ Estonia

○ Finland

○ France

○ Germany

○ Greece

○ Hungary

○ Ireland

○ Italy

○ Latvia

○ Lithuania

○ Luxembourg

○ Malta

○ Netherlands

○ Poland

○ Portugal

○ Romania
○ Slovak Republic
○ Slovenia
○ Spain
○ Sweden

20 Transparency register number

255 character(s) maximum

Check if your organisation is on the transparency register. It's a voluntary database for organisations seeking to influence EU decision-making.

53905947933-43

* 21 Country of origin

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

○ Afghanistan
○ Åland Islands
○ Albania
○ Algeria
○ American Samoa
○ Andorra
○ Angola
○ Anguilla
○ Antarctica
○ Antigua and Barbuda
○ Argentina
○ Armenia
○ Aruba
○ Australia
○ Austria
○ Djibouti
○ Dominica
○ Dominican Republic
○ Ecuador
○ Egypt
○ El Salvador
○ Equatorial Guinea
○ Eritrea
○ Estonia
○ Eswatini
○ Ethiopia
○ Falkland Islands
○ Faroe Islands
○ Fiji
○ Finland
○ Libya
○ Liechtenstein
○ Lithuania
○ Luxembourg
○ Macau
○ Madagascar
○ Malawi
○ Malaysia
○ Maldives
○ Mali
○ Malta
○ Marshall Islands
○ Martinique
○ Mauritania
○ Mauritius
○ Saint Martin
○ Saint Pierre and Miquelon
○ Saint Vincent and the Grenadines
○ Samoa
○ San Marino
○ São Tomé and Príncipe
○ Saudi Arabia
○ Senegal
○ Serbia
○ Seychelles
○ Sierra Leone
○ Singapore
○ Sint Maarten
○ Slovakia
○ Slovenia

○ Azerbaijan
○ Bahamas
○ Bahrain
○ Bangladesh
○ Barbados
○ Belarus
● Belgium
○ Belize
○ Benin
○ Bermuda
○ Bhutan
○ Bolivia
○ Bonaire Saint Eustatius and Saba
○ Bosnia and Herzegovina
○ Botswana
○ Bouvet Island
○ Brazil
○ British Indian Ocean Territory
○ British Virgin Islands
○ Brunei
○ Bulgaria
○ Burkina Faso
○ France
○ French Guiana
○ French Polynesia
○ French Southern and Antarctic Lands
○ Gabon
○ Georgia
○ Germany
○ Ghana
○ Gibraltar
○ Greece
○ Greenland
○ Grenada
○ Guadeloupe
○ Guam
○ Guatemala
○ Guernsey
○ Guinea
○ Guinea-Bissau
○ Guyana
○ Haiti
○ Heard Island and McDonald Islands
○ Honduras
○ Mayotte
○ Mexico
○ Micronesia
○ Moldova
○ Monaco
○ Mongolia
○ Montenegro
○ Montserrat
○ Morocco
○ Mozambique
○ Myanmar /Burma
○ Namibia
○ Nauru
○ Nepal
○ Netherlands
○ New Caledonia
○ New Zealand
○ Nicaragua
○ Niger
○ Nigeria
○ Niue
○ Norfolk Island
○ Solomon Islands
○ Somalia
○ South Africa
○ South Georgia and the South Sandwich Islands
○ South Korea
○ South Sudan
○ Spain
○ Sri Lanka
○ Sudan
○ Suriname
○ Svalbard and Jan Mayen
○ Sweden
○ Switzerland
○ Syria
○ Taiwan
○ Tajikistan
○ Tanzania
○ Thailand
○ The Gambia
○ Timor-Leste
○ Togo
○ Tokelau

○ Burundi
○ Cambodia
○ Cameroon
○ Canada
○ Cape Verde
○ Cayman Islands
○ Central African Republic
○ Chad
○ Chile
○ China
○ Christmas Island
○ Clipperton
○ Cocos (Keeling) Islands
○ Colombia
○ Comoros
○ Congo
○ Cook Islands
○ Costa Rica
○ Côte d’Ivoire
○ Croatia
○ Cuba
○ Curaçao
○ Hong Kong
○ Hungary
○ Iceland
○ India
○ Indonesia
○ Iran
○ Iraq
○ Ireland
○ Isle of Man
○ Israel
○ Italy
○ Jamaica
○ Japan
○ Jersey
○ Jordan
○ Kazakhstan
○ Kenya
○ Kiribati
○ Kosovo
○ Kuwait
○ Kyrgyzstan
○ Laos
○ Northern Mariana Islands
○ North Korea
○ North Macedonia
○ Norway
○ Oman
○ Pakistan
○ Palau
○ Palestine
○ Panama
○ Papua New Guinea
○ Paraguay
○ Peru
○ Philippines
○ Pitcairn Islands
○ Poland
○ Portugal
○ Puerto Rico
○ Qatar
○ Réunion
○ Romania
○ Russia
○ Rwanda
○ Tonga
○ Trinidad and Tobago
○ Tunisia
○ Turkey
○ Turkmenistan
○ Turks and Caicos Islands
○ Tuvalu
○ Uganda
○ Ukraine
○ United Arab Emirates
○ United Kingdom
○ United States
○ United States Minor Outlying Islands
○ Uruguay
○ US Virgin Islands
○ Uzbekistan
○ Vanuatu
○ Vatican City
○ Venezuela
○ Vietnam
○ Wallis and Futuna
○ Western Sahara

○ Cyprus
○ Czechia
○ Democratic Republic of the Congo
○ Denmark
○ Latvia
○ Lebanon
○ Lesotho
○ Liberia
○ Saint Barthélemy
○ Saint Helena Ascension and Tristan da Cunha
○ Saint Kitts and Nevis
○ Saint Lucia
○ Yemen
○ Zambia
○ Zimbabwe

*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

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 sub-section.
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.

3000 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

3000 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?

5000 character(s) maximum

The COVID-19 outbreak has raised many challenges across sectors (not only when it comes to the availability of illegal goods online), and EDiMA’s members have worked to address these challenges as they have manifested on their services. Some examples of the various measures taken by our members can be found here: https://twitter.com/EDiMA_EU/status/1253337897119281156.

Our members have also maintained regular dialogues with Commissioner Reynders and Commissioner Breton, who have praised the companies’ efforts to step up as responsible actors in the community.

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.

3000 character(s) maximum

Since the outbreak of the pandemic, our members have prioritized tackling coronavirus-related illegal content across their platforms. Common types of scams and illegal activities our members have encountered include:

- Sales of fraudulent products
- Posing as government sources
- Fraudulent financial offers
- Fake charitable donation requests

It is worth noting that our members have a lot of experience addressing such illegal activities and they continuously improve the ways they are addressing such content, including by utilizing automation and machine learning (where possible).

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

3000 character(s) maximum

EDiMA's members have been working tirelessly to protect users in response to the new threats arising during the pandemic. Many members collaborated closely with the European Commission's DG JUST and with competent authorities and governments across the EU. We believe that such enhanced collaboration, which is based on well-tried legal removal processes, can help tackle illegal content in future.

Over the years, members have built systems to address similar scams and misleading offers. Many online service providers provide online forms that allow competent authorities to request the removal of content that violates the laws of their country. It helps service providers if the complainant includes as detailed information about the illegal activities as possible - full page URLs, explanation why content is unlawful etc.

As an example, Google's systems have detected 18 million malware and phishing Gmail messages per day related to COVID-19 (of the more than 100 million phishing emails that Gmail blocks every day), in addition to more than 240 million COVID-related daily spam messages: https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond.

Another example, eBay has provided to the Commission with a list of policy and enforcement steps taken to address fraudulent and misleading practices on the platform arising in the Covid-19 situation (although this does not relate to illegal content per se): https://ec.europa.eu/info/sites/info/files/live_work_travel_in_the_eu/consumers/documents/ebay_-_summary_for_consumers.pdf

Some other examples can be found here: https://twitter.com/EDiMA_EU/status/1253337897119281156

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)?

3000 character(s) maximum

Depending on the nature of the service, online service providers deploy machine learning and pattern recognition software, as well as human pre- and post-moderation, plus customer service agents who can respond to complaints. They also cooperate with law enforcement agencies where appropriate.

21 Do you consider these measures appropriate?

- ● Yes
- ○ No
- ○ I don't know

22 Please explain.

3000 character(s) maximum

Initiatives are continuously evolving - they have developed over time and have adapted to emerging challenges and to technological capabilities available. There is no silver bullet, online service providers need to use a mix of technology, as well as traditional tools and approaches, often depending on the nature of their services and activities. Cooperation with other stakeholders (both online and offline) is also essential.

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.

3000 character(s) maximum

Based on how the above question is phrased, EDiMA understands it is aimed at business users, nonetheless we would like to provide information on business users whose content is either removed or blocked. It is worth noting that as laid out in the Platform-to-Business (P2B) Regulation, the provider of online intermediation services can have legitimate reasons to delist or remove certain goods or services that are considered to be illegal. In principle the suspension or termination of a business user’s account is duly notified.

However, this is not always possible as doing so could interfere with a pending investigation by competent public authorities, legal action against a business user or any measure taken to protect the end user of the platform. In these instances the service provider may not be in a position to provide a statement of reasons, as providing an overview of the ‘specific facts and circumstances’ which lead to the decision could help ill-intended business users refine their fraudulent strategy.

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.

3000 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?

3000 character(s) maximum

Yes, this is taken very seriously by online service providers (where they encounter these issues on their services). Online service providers, and indeed other stakeholders in the online ecosystem, all have a responsibility to implement proportionate measures ensuring that children are protected online. Service providers are implementing minimum age requirements, and complying with the terms of the GDPR, AVMSD, implementing parental controls, and adapting their terms of service to ensure child protection measures. Service providers also collaborate with experts to continuously develop methods for prevention, detection and enforcement (against company/ industry standards).

A major gap is still seen in adequate resources being dedicated to protection of children by public authorities in a variety of areas ranging from education and awareness raising of harmful behaviour (both online and offline) to enforcement of punitive measures against the perpetrators of illegal activities online.

That said, it is still important to register the distinction between harmful behaviours and illegal behaviours, as this sets an important legal basis from which service providers can take action. Moreover, any rules ought to be proportionate, service- and content-specific.

Finally, as to the wording of the question, what would inappropriate content mean here? And where would it fit within the spectrum of illegal and harmful content and activity? We would highlight that the term inappropriate is very subjective, and even in the offline world examples of this can be found - e.g. national broadcasting authorities receive complaints from viewers for TV programmes screened at 6pm that are regarded as “inappropriate” by some parents but are nonetheless in line with broadcasting rules.

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

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree	I don't know/ No reply
Online platforms can easily be manipulated by foreign governments or other coordinated groups to spread divisive messages	○	○	○	●	○	○
To protect freedom of expression online, diverse voices should be heard	●	○	○	○	○	○
Disinformation is spread by manipulating algorithmic processes on online platforms	○	○	●	○	○	○
Online platforms can be trusted that their internal practices sufficiently guarantee democratic integrity, pluralism, non-discrimination, tolerance, justice, solidarity and gender equality.	○	●	○	○	○	○

3 Please explain.

3000 character(s) maximum

Online service providers have shown their commitment to being part of the solution, trying to actively tackle disinformation by means of the industry Code of Practice (CoP) on disinformation and the many additional efforts they have taken in addition to their commitments in the CoP.

However, there are still gaps regarding the definition of disinformation and other definitions needed to allow the sector to act e.g. lack of clarity on electoral rules at every level in every Member State. Furthermore, experience has shown that effective interaction with other stakeholders (both from government as much as other industry stakeholders) such as the media sector is imperative to making efforts in the disinformation space successful. It is therefore essential that the Code extends to other relevant sectors too.

The legal definition of disinformation, transparency on relevant rules service providers need to take into account, and the nature of the content and the services involved will all need to be considered for any further work on disinformation.

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.

3000 character(s) maximum

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

3000 character(s) maximum

As stated above, our members have stepped up in their responses to the issues raised by the COVID-19 outbreak and have launched many specific measures to tackle harmful activities as and where they have manifested on their services. Some examples include: https://twitter.com/EDiMA_EU/status /1253337897119281156

In addition, our members have worked to collaborate with authorities at national, European and global level, e.g. the WHO to remain abreast of the latest developments regarding the pandemic and to provide insight into the initiatives that were taken by the services.

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?

5000 character(s) maximum

There is a concern with regard to erroneous removals, but this varies between online service providers and much of these issues are related to different interactions with various stakeholders and the nature of the content and goods concerned.

An example includes the relationship between online service providers and IPR owners. In this case, some of EDiMA's members have experienced numerous removals made at the request of IPR owners that have turned out to be unjustified. This occurs for a number of reasons, including bad faith notices from IPR owners seeking to stifle online trade because they prefer to keep distribution offline, enforcement of selective distribution agreements, enforcement of IPR in jurisdictions where the IP is not actually protected (e.g. countries where a trademark is not registered), good-faith errors, and attempts to reduce the availability of competing products. Additional issues can arise when larger IP owners submit overly broad removal requests, which can inadvertently result in the removal of legitimate goods and/or listings. Some members have also experienced situations in which an IP owner submits e.g. three notices in rapid succession, in order to get a seller banned from the service provider's platform.

Each of these instances has an economic impact on legitimate sellers, as well as on the relationship between the sellers and the online service provider concerned. The legal framework today does not provide strong enough disincentives to such behaviour by notice providers.

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.

3000 character(s) maximum

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

3000 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?

3000 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

7 Please provide a link to publicly available information or reports.

1000 character(s) maximum

While this question seems to be aimed more at stakeholders submitting notices to online service providers for removal of illegal content or goods/services, online service providers themselves also engage in these actions in order to increasingly ensure the safety of the services they provide. They also cooperate with supervisory authorities and respond to requests for information in line with national and EU rules, all as part of a broader effort to act in good faith and ensure the safety of their users.

Some examples of transparency reports then include:
Facebook: https://transparency.facebook.com/
Google: https://transparencyreport.google.com/about?hl%3Den_GB&sa=D&ust=1598521334333000&usg=AFQjCNFBFzZAdZ_UBe5935dn_GF53psT6Q

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?

3000 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 ar you aware of alternative sources of such data? Please explain.

3000 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.

5000 character(s) maximum

Our members use numerous techniques and methods, and a combination of the above. A range of tools and approaches is necessary, and the most effective combination will depend on different factors such as type of illegal content/activity, the nature of the service, the volume of complaints and sector, etc. Other stakeholders also have a part to play in tackling illegal activities online, cooperation is essential.

Furthermore, it is important that there are safeguards in place, to ensure legal certainty to allow online service providers to act.

3 What issues have you encountered in operating these systems?

5000 character(s) maximum

Our members have encountered a variety of issues, including (but not limited to):

- Bad quality notices or data in notices;
- Erroneous, fraudulent and abusive notices;

- Errors by automated reporting;
- Delayed reporting;
- Poor resources in police departments (outdated technology, limited understanding of digital world);
- Insufficient expertise in judiciary (leading to case law that affects the operation of systems);
- Ambiguity on what constitutes unlawful;

Another example can arise in situations in which notices are submitted on behalf of a company by a third party service. In these cases, perverse incentives can be created where the third party's remuneration from the company is tied directly to the number of notices they submit on their behalf - which can lead to the submission of too many inaccurate notices tied to volume rather than quality.

It is also important to bear in mind that the technological tools employed are still not capable of identifying and removing illegal content exhaustively and accurately. There are also challenges to be factored in when it comes to the mental health of human moderators, which companies actively and continuously address by putting in place robust systems to ensure the health and safety of their moderators. Other challenges to be considered include bad faith on the part of users, and third parties (e.g. brand owners) using online service providers as a dispute resolution system. Inadequate access to public resources is also an issue (e.g. certain national databases of registered dog breeders, car history data, etc.) - which again points to the importance of cooperation among stakeholders when approaching these issues online.

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.

5000 character(s) maximum

This is difficult, if not impossible to quantify. There are a number of considerations to take account of when forecasting content moderation costs and specifically costs related to "notice and action".

Firstly, developing and drafting clear, fair policies and enforcement strategies is resource intensive - often service providers will invest in significant research and consult with outside experts when developing these policies and strategies, and this initial investment needs to be kept in mind as part of the overall cost.

Next, a lot of content moderation still depends on human review in many, if not most, circumstances. Staffing this work is one of the greatest challenges, particularly for small and medium sized service providers. This is why we do not believe having human content moderators should be a legal obligation, except potentially for the most high risk types of illegal content and higher risk of exposure. Instead, any obligation in this respect should be proportionate, so that a service provider can align their costs where there are the most risks involved.

Where AI tools are employed, online service providers must continuously invest to optimise and improve these tools, and/or also employ external tools that assist them in identifying infringing content (e.g. image search software). Such IT infrastructure is costly to operate and adapt to evolving trends, taking account of the staffing and engineering costs that will necessarily be involved - as mentioned above. This is an asymmetric contest with bad actors that are continually looking for techniques to evade these controls and as such they need continual review and audit as to the false positive/false negative rates that they produce. It is not a simple “invest, deploy and forget” situation. This point was explored extensively during the debates on the Copyright Directive, and it is the case for technical tools for all types of content.

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.

5000 character(s) maximum

Many of our members publish transparency reports on their enforcement efforts. Some examples of which include:

Airbnb:
https://news.airbnb.com/transparency/

Etsy (2019):
https://extfiles.etsy.com/advocacy/Etsy_2019_Transparency_Report.pdf.

Facebook:
https://transparency.facebook.com/

Google and YouTube:
https://transparencyreport.google.com/; https://transparencyreport.google.com/youtube-policy/removals; https://www.blog.google/products/ads/stopping-bad-ads-to-protect-users/; https://transparencyreport.google.com/political-ads/home

Mozilla:
https://www.mozilla.org/en-US/about/policy/transparency/

Verizon Media:
https://www.verizonmedia.com/transparency/index.html

Based on our members’ experience with annual transparency reports, there are a few points we would highlight going forward when considering any specific rules on transparency reporting:

- There should not be an obligation on service providers to report on the exact types of automated tools used or the details of their functionalities. Transparency around outcomes and actions can still be useful, but disclosing too much about how a service provider takes a particular enforcement action can inadvertently provide a guide to bad actors to game their systems.
- Any specific rules on the frequency of transparency reports will require operational changes from service providers, which may be too burdensome for some service providers. Furthermore, should reports be requested too frequently they could be ineffective as it will be impossible to analyse the data and to draw conclusions within unrealistic timelines.
- Regarding the content of any transparency reports, we would advise against the consideration of any horizontal template for transparency reporting across businesses and online service providers - as this will not achieve the desired effect and will not sufficiently take account of the nuances of different service offerings. Proportionality should instead be the key indicator for transparency reports going forward.
- There should not be obligations on the service provider to provide detailed reporting on the status of

different user flags and notices. Many user flags are inaccurate or abusive, and a service provider needs to be flexible in its response to take account of these challenges. Rules on reporting the exact turn around time of flags, or information about each step in the process for each flag would hamper this flexibility.

A final point, we are not aware of similar transparency reports being made available from parties submitting such notices. We believe it would be useful to have more information on where notices are filed, the numbers, the rejection rates and the sort of issues notified (e.g. types of rights, goods and content, infringement in question) - to enhance cooperation among stakeholders and optimise notice and action procedures.

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)?

3000 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.

5000 character(s) maximum

Depending on the online service provider, the types of services they provide and on their own Terms of Service (ToS), some or all of the above are covered. That said, the word “ban” used in the above question can be misleading, as in practice there are national rules and rules relating to different jurisdictions which also need to be considered.

Different measures taken against content/activity which might be harmful but are not illegal will then usually depend on the nature of the service and the type of harms encountered on that service. An online service provider has a legal obligation to take action when it is made aware of illegal content/activity on its service, but often any action on “harmful” content will be based on the service provider’s ToS. Terms of service are often used to specify which types of content and activity a service provider will allow, and can be a complementary enforcement tool which can often adapt well to some of the issues faced online when it comes to harmful content.

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

3000 character(s) maximum

We are not sure whether this question relates to the possibility for users to report “harmful” content/activity to the service provider, or to service providers’ reporting to enforcement authorities.

Service providers have different systems in place for users to report “harmful” activities, depending on the nature of the content, the nature of their service, and the rules of their terms of service.

When it comes to service providers’ proactive reporting to e.g. law enforcement, these systems are different per country. If content is legal it is harder to justify reporting it. For service providers to take action a framework is needed, clearer legal definitions and certainty is essential to make it possible for services to act.

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

5000 character(s) maximum

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

5000 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.

3000 character(s) maximum

If/when minors could be exposed to risks through the use of certain activities/services online, different online service providers have developed specific policies according to their service offerings. For example:

● The industry's work to report content via National Center for Missing & Exploited Children (NCMEC), which then sends reports to law enforcement agencies: http://www.missingkids.com/home

● Company policies to prevent sexualisation of minors, harmful or dangerous acts involving minors, inflicting emotional distress and cyberbullying and harassment of minors.

More specifically, some companies have developed technologies which they share with industry, such as:

- https://protectingchildren.google/intl/en/
- CSAI match: https://youtube.com/csai-match/
- Content Safety API: https://www.blog.google/around-the-globe/google-europe/using-ai-help-organizations-detect-and-report-child-sexual-abuse-material-online/
- Tools like Family Link (https://families.google.com/familylink/) to keep parents in the loop.

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?

5000 character(s) maximum

Members do have counter-notice options in the event of user disputes, but these raise their own challenges too. For example, with counter-notice systems on illegal content there is a risk that a user's dispute will make a service provider become the arbitrator between the original complainant and the content uploader, in cases where the service provider does not have all of the facts. There is also a risk that a service provider receives an invalid counter-notice or that a user misrepresents themselves in a counter-notice.

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?

3000 character(s) maximum

When it comes to automated detection and/or removal tools, many service providers have (to varying degrees, depending on the service and their resources) some combination of human and machine oversight in place. We would continue to stress that automated content recognition systems are not perfect and are not effective for many types of content. They also cannot recognise context or assess use cases when it comes to making decisions on the illegality of a piece of content for example. This means that the people and machines combination is typically required, but the costs associated with it can be very burdensome as this must incorporate not only continuous software updates to automated systems (to train the tech to adapt to users trying to game the system) as well as training and resources for human moderators (who can also be susceptible to bias). See more details on the limits of automated content recognition technology in additional responses below.

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

○ Yes

○ No

5 Please explain.

5000 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.

5000 character(s) maximum

Bearing in mind the diversity of services and business models of EDiMA members we would like to point out that a level of flexibility and proportionality is needed to allow for relevant reporting.

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?

5000 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.

5000 character(s) maximum

These cases can be very different depending on the online service provider, some examples include:

- Participation in the Hate Speech Code of Conduct;
- The Global Internet Forum to Counter Terrorism (GIFCT) including sharing hashes with other industry partners;
- Sharing child sexual abuse material data with NCMEC (third party clearinghouse, which then sends to law enforcement);
- Reports of removal requests sent to the Lumen Database.

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	Yes, only by	Yes, only platforms at particular risk of	Such measures should not be

	they intermediate (e.g. content hosting, selling goods or services)	larger online platforms	exposure to illegal activities by their users	required by law
Maintain an effective ‘notice and action’ system for reporting illegal goods or content	●	○	○	○
Maintain a system for assessing the risk of exposure to illegal goods or content	●	○	○	○
Have content moderation teams, appropriately trained and resourced	○	○	○	●
Systematically respond to requests from law enforcement authorities	○	○	○	●
Cooperate with national authorities and law enforcement, in accordance with clear procedures	○	○	○	●
Cooperate with trusted organisations with proven expertise that can report illegal activities for fast analysis ('trusted flaggers')	○	○	○	●
Detect illegal content, goods or services	○	○	○	●
In particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law	○	○	○	●
Request professional users to identify themselves clearly (‘know your customer’ policy)	●	○	○	○
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)	○	○	○	●
Inform consumers when they become aware of product recalls or sales of illegal goods	●	○	○	○
Cooperate with other online platforms for exchanging best practices, sharing information or tools to tackle illegal activities	○	○	○	●

Be transparent about their content policies, measures and their effects	●	○	○	○
Maintain an effective ‘counter-notice’ system for users whose goods or content is removed to dispute erroneous decisions	●	○	○	○
Other. Please specify	○	○	○	○

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

5000 character(s) maximum

● A general remark to the framing of the above questions, the broad reference to ‘platforms’ can be misleading and does not provide sufficient nuance in the approach and assessment of the issues in question.

● We support voluntary approaches for some of the points above where we oppose them being made into legal requirements.

● Having teams in place for content moderation should not be a legal requirement as it greatly depends on the nature of the service and exposure to risks by users.

● We do not think trusted flaggers should be legally required, their involvement depends on whether it works for the business or service in question.

● The detection of illegal content and goods should not be legally required either. While online service providers can (and often do) proactively search for illegal content and goods in good faith, a legal requirement to proactively do so would amount to a legal requirement to seek facts or circumstances relating to illegal activity, which is in contradiction to the Article 15 of the e-Commerce Directive.

● Regarding the point on informing professional users on EU law obligations, we do not think this should be a legal requirement either - for the same reason that this would qualify as seeking facts or circumstances indicating illegal activity under Article 15 of the e-Commerce Directive.

● On the need to clarify notice and actions policies, this should refer to services provided rather than platforms - as platforms can provide many different types of services.

● Regarding the points on systemically responding to law enforcement authorities and cooperation with national authorities, we understand the legitimate interests of law enforcement, but we would be concerned about proposals that would circumvent existing legal protections or require online service providers to disclose user data to the government without any prior oversight by an independent authority and without proper safeguards.

● On the “know your customer” obligation, while in principle it could contribute to ensuring safety on marketplaces, any new measure in this direction must be privacy-friendly, proportionate and supported by the right infrastructure in order to be scalable, while enabling the businesses of all sizes to thrive. To allow a service provider to effectively check a “professional user’s” identity, any verification should be done against publicly available databases. It is also important that any data collection and verification requirement should be limited to what is reasonably necessary and proportionate to achieve the intended goals. Moreover, since the process of screening sellers against publicly available databases for KYB/C purposes can be costly and operationally burdensome, service providers should be empowered to adopt a risk-based approach to determine the cadence for rescreening. For example, professional users could be screened during their initial onboarding onto a service, while more “high-risk” professional users could be rescreened on the basis of objective criteria such as e.g. country of location, category of products sold etc.

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

3000 character(s) maximum

● On the precise location, the URL is just one example of how precise location can be identified. Others include video timestamps, or other unique identifiers.

● Proof/evidence of relevant (IP) rights, standing, expertise is also required. In this context, an explanation of how the relevant content infringes law, T&Cs, and/or 3rd party rights is also necessary.

● A statement of the good faith and validity of the claim is required to deter bad-faith notices.

● In the case of the identity of the person or organisation, there are of course exceptions - anonymous notices can be sent, e.g. when the notice provider might be incriminating him/herself or is worried about retaliation or their own safety.

● A notice must also always be submitted through the proper specified channels in order to be considered valid.

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

5000 character(s) maximum

Notice and action (N&A) remains the most horizontally workable approach across business models and services. In the recently adopted Copyright Directive, Recital 66 acknowledges that in many cases due to technological limitations, notice and action will be the only possible recourse for content that reappears that is illegal. New framework should be drafted with the current legal framework in mind and should not undermine it.

For many of our members, a combination of notice and action, automated systems and human review is deployed. These systems are never 100% accurate and often our members' actions are based on voluntary efforts to address issues identified with illegal content on their services, which is why we continue to advocate for legal safeguards to ensure that service providers do not automatically face a loss of their limited liability protection under the e-Commerce Directive for any voluntary actions they take to address these concerns.

We would particularly oppose the creation of a “take down and stay down regime”, as this would require an online service provider to seek out illegalities on a continuous basis. Not only would this be incompatible with Article 15 of the e-Commerce Directive, it is currently not a workable standard for most service providers. Such an approach would require the deployment of costly automated tools, the most accurate of which only exist today for certain types of content (audio and audiovisual) and which can still result in errors and false flags as they cannot identify context and legitimate uses of content. To encourage a take down and stay down regime would moreover be disproportionate, as it would encourage service providers to error on the side of caution and adopt the use of any possible automated tools to comply with this standard, which will inevitably infringe on users' fundamental rights.

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?

3000 character(s) maximum

Errors in takedowns and impact on freedom of expression are the main risks associated with the use of automated tools.

Automated tools cannot recognise context, and can often result in the removal of perfectly legitimate content. For example, content that appears similar or even appears identical is often different in material aspects to a machine. The best known examples are photographs which are visually identical but have entirely different digital signatures. This means that automated tools are slightly more useful in clear cut situations where there are very clear definitions and content and activity that is unambiguously illegal - so for example, in cases involving the use of certain words or imagery in high-threshold contexts (e.g. CSAM material) - but even these scenarios can result in errors. This is also why the use of automated tools should not be mandated, and it is essential that any requirement to remove illegal content (via any tools) under the DSA is grounded in very clear legal definitions.

Cooperation is something to be considered when examining the use of automated tools as well - they are reliant on information (hash databases, fingerprints, etc.), and the more access to information about different types of content a service provider has, the more the tools can pick up. Sharing resources and database for some types of illegal content can be helpful here - for example, the Global Internet Forum to Counter Terrorism has established a hash sharing database for illegal terrorist content, to optimise removals across different online services.

Finally, automated tools are also very costly to develop and maintain, and still require human review - even where content is initially flagged by an automated tool, often a human will be somewhere in the loop either to review the decision or where a user contests the decision. This requires a further commitment of resources and the costs associated. While automated tools offer promise for content moderation at scale in the future, it is important for policymakers to understand that developing, implementing, and iterating effective tools requires significant resources and machine learning capabilities, which may be out of reach for new startups looking to compete with larger players in the space.

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?

3000 character(s) maximum

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.?

5000 character(s) maximum

We continue to support a graduated intermediary liability system that recognizes the important distinctions between services, as set out in the e-Commerce Directive. The main definitions of the e-Commerce Directive remain relevant, and enforcement should tend towards targeted removal at source rather than down-stack intervention. Down-stack interventions (e.g. aimed at ISPs, IaaS, browsers) are more rights-interfering and especially for the transport layer, easily circumventable.

A general remark on the framing of the question, what is meant by the reference to “online platforms” in this question? This is a very broad reference which encapsulates many of the different online service providers listed.

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?

5000 character(s) maximum

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?

5000 character(s) maximum

It is important for policymakers to consider strategies to stop the spread of illegal content separately from those meant to curb harmful content. Any addition of new responsibilities in the DSA framework should not include specific obligations to remove or filter harmful content that is not illegal. In fact, we would argue that the DSA should initially focus on getting the framework right to address illegal content and activity, where there is more legal certainty upon which to base new rules and systems. EDiMA members are committed to continued and open dialogue with the Commission on effective ways to address harmful content that is not per se illegal.

Context is important when it comes to assessing content that is harmful but not illegal. Moreover, content that is appropriate on some services may be inappropriate on others; what may be appropriate for some users may be inappropriate for others. Therefore service providers are themselves best-placed to address how to respond to these issues with “harmful” content in line with variations in national Member State laws and in line with their own terms of service and subject to the laws of their relevant jurisdictions. Enforcing clear terms of service is a legitimate way for service providers to pursue issues they have noted on their service with content that is harmful but not illegal, without crossing into quasi-enforcement or judicial functions. The continued application of robust notice and action regimes for the enforcement of these terms of service will help in this area, particularly where service providers can increasingly work with trusted partners to flag different types of “harmful” content. Service providers can also use different tools to reduce the proliferation of content they have identified as “harmful” in line with their terms of service, for example by adapting the algorithms of a service to reduce the reach and influence of harmful content, or by limiting access to certain functions on the service where harmful content is identified (for example, by eliminating access to profanity in auto-complete typing). Ultimately, this approach prevents the spread of harmful content, while avoiding censoring speech.

In this regard, safeguards are clearly needed to ensure that these voluntary proactive actions taken by service providers do not automatically lead to a loss of their limited liability protection under Article 14 of the e-Commerce Directive.

Better cooperation with national authorities will also help to facilitate proportionate and appropriate responses to issues with harmful content.

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.

5000 character(s) maximum

Service providers can be encouraged to design and put in place systems to help address issues they have noted that arise from the presence of harmful content on their services. It is for this reason that we advocate for safeguards under the DSA for service providers which make voluntary efforts to address concerns on their services without fearing an automatic loss of their limited liability protections under the eCD. Where specific issues have been identified relating to harmful content or content concerning minors, legislation could provide the necessary legal certainty.

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	○	○	○	●	○	○
Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with user complaints	○	○	○	●	○	○

Tackle the use of fake-accounts, fake engagements, bots and inauthentic users behaviour aimed at amplifying false or misleading narratives	○	○	○	●	○	○
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	○	○	○	●	○	○
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	○	●	○	○	○	○
Adapted risk assessments and mitigation strategies undertaken by online platforms	○	○	●	○	○	○
Ensure effective access and visibility of a variety of authentic and professional journalistic sources	○	○	○	●	○	○
Auditing systems for platform actions and risk assessments	○	○	●	○	○	○
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.	○	○	●	○	○	○
Other (please specify)	○	○	○	○	○	○

13 Please specify

3000 character(s) maximum

Online service providers have shown their commitment to being part of the solution, trying to actively tackle disinformation by means of the industry Code of Practice (CoP) on disinformation and the many additional efforts they have taken in addition to their commitments in the CoP. Whereas many of the measures described in the table above are effective none of them should be prescribed to all services, as the experience of the CoP has demonstrated the measures need to be tailored to the type of service and the service infrastructure.

Furthermore, there are still gaps regarding the definition of disinformation and other definitions needed to allow the sector to act e.g. lack of clarity on electoral rules at every level in every Member State. Furthermore, experience has shown that effective interaction with other stakeholders (both from government as from other industry stakeholders) such as the media sector is imperative to making efforts in the disinformation space successful. It is therefore essential that the Code extends to other relevant sectors too.

The legal definition of disinformation, transparency on relevant rules service providers need to take into account, and the nature of the content and the services involved will all need to be considered for any further work on disinformation.

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?

3000 character(s) maximum

Crises cannot be anticipated, so flexibility is needed. The COVID-19 health crisis has amplified the need for digital services to cooperate effectively with authorities and third party experts. Collaboration with responsible authorities, ongoing dialogues on methods, and establishing connections where any authoritative content needs to be promoted – these are all tools that should be continuously considered, so that there is a sound underlying structure to address certain issues when a crisis develops. In addition, third party experts are not only essential to identify all forms of illegal content, but they will also have the expertise to identify important trends and emerging threats to the public, for example in a health crisis.

Next, in order for online service providers to react quickly to notices when such a crisis emerges, it’s essential to ensure that a clear and harmonised notice and action regime is in place, where notices are submitted with all the relevant information and online service providers are clear on what constitutes a valid notice and who can submit a valid notice.

Finally, legal safeguards which allow companies to take more proactive good-faith actions to address concerns as they manifest on a service are also needed. Good faith cooperation between online service providers and public authorities is also key to ensure the success of such mechanisms.

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	○	○	○	●	○	○
Diligence in assessing the content notified to them for removal or blocking	○	○	○	●	○	○
Maintaining an effective complaint and redress mechanism	○	○	○	●	○	○

Diligence in informing users whose content/goods/services was removed or blocked or whose accounts are threatened to be suspended	○	○	○	●	○	○
High accuracy and diligent control mechanisms, including human oversight, when automated tools are deployed for detecting, removing or demoting content or suspending users’ accounts	○	○	●	○	○	○
Enabling third party insight – e.g. by academics – of main content moderation systems	○	○	●	○	○	○
Other. Please specify	○	○	○	○	○	○

16 Please explain.

3000 character(s) maximum

Service providers take a variety of steps to ensure the protection of the freedom of expression of their users, which are also developed in light of the idiosyncrasies of their specific services.

But with any of these steps, service providers need to be allowed adequate time/flexibility to make sound determinations on content removals, and as such any provisions in the DSA regarding content removal ought to avoid introducing strict turn-around times.

Online Service providers also need to be allowed adequate flexibility in the mechanisms they deploy, to allow them to respond in a manner that ensures a fair process and outcome. For example:
(1) Maintaining an effective complaint and redress mechanism.
(2) Establishing effective and accurate control mechanisms, including human oversight, when using automated tools to detect, remove or demote content, or suspend users’ accounts.
(3) Informing and providing explanations to users whose content/goods/services are removed or whose accounts are threatened with suspension.

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?

5000 character(s) maximum

Bearing in mind the diversity of businesses that will be complying with the DSA, all requirements under the DSA should be easy to implement, transparent and workable for businesses regardless of their size.

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.

5000 character(s) maximum

In general, it is important to have clear content policies, systems for reviewing user flags of content, and a system to notify users when their content has been removed with an opportunity to appeal.

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?

5000 character(s) maximum

There is a need to balance transparency and information that is in the public interest (e.g. to demonstrate that tackling illegal activity is a focus for the online service provider, that appropriate resources are allocated, and what categories of violative content are prevalent on a given platform) with feasibility (e.g. there may be limitations on the type of data collection and analysis available to the online service providers, particularly smaller service providers). We also caution against making details regarding automated controls available to the public or users, as such information would enable bad actors to circumvent our controls. We would encourage, however, collaboration between competent authorities and online service providers to ensure automated controls keep pace with emerging threats.

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

5000 character(s) maximum

Users should be given a general understanding of how the algorithm works to help them find content that is relevant to them, as is already required by the GDPR. No further regulation is therefore necessary.

It is also important to understand that disclosing the underlying algorithms could open up such systems for abuse and risks to trade secrets.

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?

5000 character(s) maximum

We generally recognise the benefit of better cooperation with authorities, including when it comes to data sharing for specific purposes. It is also important that any data sharing in this sense should be limited to what is reasonably necessary and proportionate to achieve the intended goals. However, the DSA is perhaps not best placed to legislate on data sharing agreements between online service providers and authorities. For the purposes of tax collection, for example, the Commission has recently issued a legislative proposal for administrative cooperation, and this issue should be tackled within that context to avoid legal complexity.

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)?

5000 character(s) maximum

24 Are there other points you would like to raise?

3000 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 hos the current liability exemption regime is working and the areas where an update might be necessary.

1 How important is the harmonised liability exemption for users’ illegal activities or information for the development of your company?

Please rate from 1 star (not important) to 5 stars (very important)	★★★★★

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.

5000 character(s) maximum

The categories in themselves make sense, but there are many more actors and services today in the supply chain of online services which would fall into different sub-categories of these three – it is very difficult to define where new services fall or will fall and we don’t necessarily think this is the question, rather there needs to just be a proportionate responsibility for the actors in the ecosystem.

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?

5000 character(s) maximum

CJEU case law has provided further clarification of key elements. These elements under the eCD are moreover modelled on tort law secondary liability - under this system knowledge is applied on a case-by-case basis based on an objective test, and this approach has functioned well under the current framework.

However, a level of ambiguity remains regarding the concept of actual knowledge. In order to reflect the reality of today’s services and to build on the work of the CJEU, the DSA should move away from the “mere technical, automatic and passive nature” distinction and build on the notions of actual knowledge.

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.

5000 character(s) maximum

Today, any proactive action (i.e. action undertaken voluntarily and not in response to a notice) on the side of the online service provider could result in the loss of their limited liability status. Any reform should provide safeguards against this potential loss of limited liability, to encourage hosting providers to take proactive measures. The proactive measures taken by the online service providers can be evaluated by an independent governance body, and a service provider can still be deemed to have lost its limited liability protection where it fails to take expeditious action on any illegal content for which it has received a valid notice.

The DSA should moreover incentivise all parties in the online ecosystem, including users, law enforcement, and third parties, to hold some portion of responsibility for fostering safety online. Users must hold primary responsibility for complying with the laws that govern their actions, and Member States and law enforcement have a duty to enforce and follow up on these rules.

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) is sufficiently clear and still valid? Please explain.

5000 character(s) maximum

No, today’s reality is that this distinction, developed in some case law, has caused significant uncertainty and liability risk for common features of current services. It is for this reason that the CJEU has made actual knowledge the decisive factor in its deliberations. For example in the Peterson v. YouTube case, the Advocate General’s Opinion states that only when a host acquires “intellectual control” of the information, and hence “appropriates” that information can it be said to be playing an active role sufficient to give it the appropriate level of knowledge or awareness (cf. para 152). Equally, in general, the appropriate level of knowledge or awareness must be knowledge or awareness of the specific unlawful information in issue, not general or abstract knowledge or awareness (cf. paras 171-172).

In order to reflect the reality of today’s services and to build on the work of the CJEU, the DSA should move away from the “mere technical, automatic and passive nature” distinction and build on the notions of actual knowledge.

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.

5000 character(s) maximum

The prohibition on general monitoring is essential to protect fundamental rights online, and it should be maintained in the new DSA framework. However, the debate around recent regulatory instruments (e.g. Directive on Copyright in the DSM) has brought into question the distinction between a general monitoring obligation and a specific monitoring obligation. But there is no legal definition of what a “specific monitoring obligation” might be. Unfortunately, so-called specific monitoring obligations can become de facto general monitoring requirements. These obligations carry significant risks of overblocking, disproportionately undermine fundamental rights and could threaten the freedom to conduct business by leading service providers to restrict the content base or limit permissible speech.

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

5000 character(s) maximum

No, however the DSA provides an opportunity to create a stronger responsibility framework as opposed to focusing on liability after the fact. Furthermore, we would like to point out that the liability of other stakeholders in the ecosystem should also be considered.

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 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' 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
.

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

			Neither agree			I don't

	Fully agree	Somewhat agree	not disagree	Somewhat disagree	Fully disagree	know/ No reply
Consumers have sufficient choices and alternatives to the offerings from online platforms.	○	○	○	○	○	○
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”).	○	○	○	○	○	○
It is easy for individuals to port their data in a useful manner to alternative service providers outside of an online platform.	○	○	○	○	○	○
There is sufficient level of interoperability between services of different online platform companies.	○	○	○	○	○	○
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.	○	○	○	○	○	○
It is easy for innovative SME online platforms to expand or enter the market.	○	○	○	○	○	○
Traditional businesses are increasingly dependent on a limited number of very large online platforms.	○	○	○	○	○	○
There are imbalances in the bargaining power between these online platforms and their business users.	○	○	○	○	○	○
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.	○	○	○	○	○	○
Certain large online platform companies create barriers to entry and expansion in the Single Market (gatekeepers).	○	○	○	○	○	○
Large online platforms often leverage their assets from their primary activities (customer base, data, technological solutions, skills, financial capital) to expand into other activities.	○	○	○	○	○	○
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.	○	○	○	○	○	○

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	☆ ☆ ☆ ☆ ☆
Wide geographic coverage in the EU	☆ ☆ ☆ ☆ ☆
They capture a large share of total revenue of the market you are active/of a sector	☆ ☆ ☆ ☆ ☆
Impact on a certain sector	☆ ☆ ☆ ☆ ☆

They build on and exploit strong network effects	☆☆☆☆☆
They leverage their assets for entering new areas of activity	☆☆☆☆☆
They raise barriers to entry for competitors	☆☆☆☆☆
They accumulate valuable and diverse data and information	☆☆☆☆☆
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

3000 character(s) maximum

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

3000 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 steengthen 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 - 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

1000 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).

5000 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?

5000 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).

5000 character(s) maximum

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

3000 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?

5000 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?

5000 character(s) maximum

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

3000 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?

3000 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?

3000 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.

3000 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

3000 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.

3000 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.

3000 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.

3000 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.

3000 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

3000 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.

3000 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?

3000 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.

3000 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?

3000 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?

3000 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?

3000 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?

3000 character(s) maximum

25 Taking into consideration the parallel consultation on a proposal for a 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	○	○	○	○	○	○
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	○	○	○	○	○	○
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	○	○	○	○	○	○
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.	○	○	○	○	○	○
5. There is a need for combination of two or more of the options 2 to 4.	○	○	○	○	○	○

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.

3000 character(s) maximum

27 Are there other points you would like to raise?

3000 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 though 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?

3000 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?

3000 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 though 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?

3000 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.

3000 character(s) maximum

Most of EDiMA members relying on advertising are also members of specific schemes and guiding principles such as the ones from the European Interactive Digital Advertising Alliance (EDAA) (https://www.edaa.eu/what-we-do/european-principles/).

Depending on the service, there are opportunities for consumers to tailor the advertising offered to them. Additionally, the GDPR requires companies to provide consumer control of data use.

Other models such as subscriptions depend widely on the nature of the service and the audience.

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.

3000 character(s) maximum

Yes, as reported in the context of the Code of Practice on Disinformation.

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

3000 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?

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 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 ?

3000 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?

3000 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?

3000 character(s) maximum

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

3000 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.

3000 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.

3000 character(s) maximum

5 Are there other points you would like to raise?

3000 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?

3000 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?

3000 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?

3000 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?

3000 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.

3000 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?

3000 character(s) maximum

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

3000 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.

3000 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.)

3000 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	○	○	○	○	○	○
Flexibility of choosing when and /or where to provide services	○	○	○	○	○	○
Transparency on remuneration	○	○	○	○	○	○
Measures to tackle non-payment of remuneration	○	○	○	○	○	○
Transparency in online ratings	○	○	○	○	○	○
Ensuring that individuals providing services through platforms can contact each other and organise themselves for collective purposes	○	○	○	○	○	○
Tackling the issue of work carried out by individuals lacking legal permits	○	○	○	○	○	○
Prevention of discrimination of individuals providing services through platforms, for instance based on gender, racial or ethnic origin	○	○	○	○	○	○
Allocation of liability in case of damage	○	○	○	○	○	○
Other, please specify	○	○	○	○	○	○

33 Please explain the issues that you encounter or perceive.

3000 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.

3000 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?

3000 character(s) maximum

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

through online platforms?	☆☆☆☆☆
in the offline/traditional economy?	☆☆☆☆☆

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

3000 character(s) maximum

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

3000 character(s) maximum

40 Are there other points you would like to raise?

3000 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*’.

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

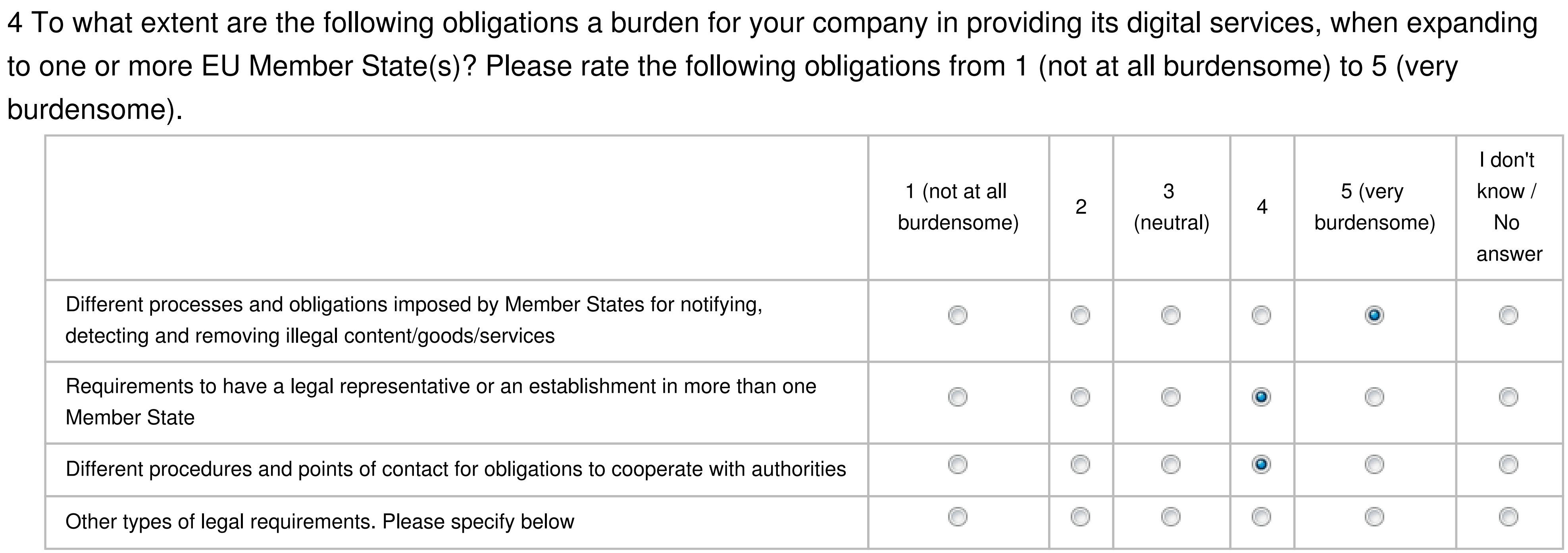
3 Approximately, what share of your EU turnover is generated by the provision of your service outside of your main country of establishment in the EU?

○ 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	○	○	○	○	●	○
Requirements to have a legal representative or an establishment in more than one Member State	○	○	○	●	○	○
Different procedures and points of contact for obligations to cooperate with authorities	○	○	○	●	○	○
Other types of legal requirements. Please specify below	○	○	○	○	○	○

5 Please specify

3000 character(s) maximum

On different Member State processes, the complexity of complying with fragmented national rules can be unduly burdensome, and makes compliance challenging for service providers. Different rules are also confusing for users.

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?

3000 character(s) maximum

Despite the existence of the Country of Origin principle, many online service providers are still struggling with significant regulatory fragmentation across the EU.

Often, Member States (and even local governments in member states) who wish to enforce obligations against online service providers as an exception to the Country of Origin principle do not notify the Member State of Origin or the European Commission of their intentions, as envisaged in the eCD. This is especially problematic in cases where local rules contradict or contravene fundamental EU legal frameworks, for example the free movement of information society services in the eCD. In this situation, there is no effective oversight of the demands being made on online service providers (or the users of the services) and therefore no ability to enter into dialogue to resolve those inconsistencies.

The DSA presents an opportunity to further clarify how the Country of Origin principle works in practice - including how and when derogations might apply - to ensure that the appropriate guidance and guardrails are in place to support local rules that are clear, fair and proportionate, whilst recognising our own obligations and responsibilities as online service providers.

Additionally, for the DSA to be truly effective, efforts should also be made to link it to the EU's Internal Market Strategy more broadly speaking - for example, the Services Directive (Directive 2006/123/EC) can be very important for online service providers operating in the EU whose services also include an offline element.

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

3000 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?

5000 character(s) maximum

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 don't know / No answer
Clearly assigned competent national authorities or bodies as established by Member States for supervising the systems put in place by online platforms	○	○	●	○	○	○
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.)	○	○	●	○	○	○
Cooperation mechanism with swift procedures and assistance across national competent authorities across Member States	○	○	●	○	○	○
Coordination and technical assistance at EU level	○	○	●	○	○	○
An EU-level authority	○	○	●	○	○	○
Cooperation schemes with third parties such as civil society organisations and academics for specific inquiries and oversight	○	○	●	○	○	○
Other: please specify in the text box below	○	○	●	○	○	○

3 Please explain

5000 character(s) maximum

Firstly, to honour the spirit of the e-Commerce Directive’s single market focus, an oversight body should function as an EU-level coordination mechanism for designated national authorities capable of delivering legal certainty and consistency for all parties.

Next, the benefit of an oversight body (whether new or an extension of an existing body) would be in their ability to provide guidance and oversight for service providers on adherence to their responsibility, and to ensure service providers are indeed taking reasonable, feasible, and proportionate measures. Crucially, the focus of an oversight body’s work should be restricted to the broad measures which service providers are taking – it should not have the power to assess the legality of individual pieces of content and it should not be empowered to issue takedown notices, which is the remit of the courts. Such competences call into play multiple critical constitutional and procedural questions, which are best left to the courts.

Finally, it should be co-regulatory in nature, such that there would be a clear consultative role for industry and civil society in its work. It would need to be staffed with technical and policy experts, to ensure the guidance and best practice it issues confirms to the spirit of the framework of responsibility. The potential oversight body should also borrow governance best-practices from existing oversight bodies in the tech sector and elsewhere – for instance, ENISA’s permanent stakeholder group, the concept of industry-driven codes of conduct overseen by data protection authorities, etc.

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

3000 character(s) maximum

The competent authorities should make publicly available information that allows:

- Citizens and users of online services to understand the rules that are being applied by the authorities, through communications that are accessible and can be understood by the general public;
- Industry and stakeholders from civil society to participate in regulatory processes;
- And, regulated entities to understand what is required of them.

Any information made available should respect the legitimate interests of regulated entities and users, including privacy, data protection and the protection of business secrets.

We think that the Commission should also be considering the accessibility and reach of information, given the various constituencies (i.e. the general public and civil society, in addition to industry) who will also benefit from such information sharing.

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

3000 character(s) maximum

It is important that competent authorities have a robust understanding of the markets they are regulating, and it may be worth exploring initiatives with industry and civil society to educate regulators and policymakers within the EU e.g., through partnerships with industry and civil society to provide market and technical education and training.

Competent authorities must also regulate from a strong evidence base, and, as in other regulatory systems, have expert legal, technical, and economic functions.

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

3000 character(s) maximum

EDiMA members all have a legal establishment in the EU and are therefore subject to comply with EU rules and regulation. Services specifically targeting EU citizens should also comply with EU rules and regulation and should therefore also be subject to oversight by the governance structure.

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

3000 character(s) maximum

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?

3000 character(s) maximum

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.

3000 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.

3000 character(s) maximum

Given that the implementation deadline for the revised AVMSD has not yet passed, it is too early to assess the overall efficiency of ERGA’s new role in cooperation mechanisms in cross border cases.

However, we welcome the possibility for ERGA mechanisms to support consistency in national approaches, especially where, because of the operation of CoO, channel owners and service providers may be subject to different rules. E.g. if ERGA produced guidance on age-gating measures, this would promote consistency in transposition and enforcement across Europe, and reduce the risks to users from an inconsistent experience.

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)

3000 character(s) maximum

14 Are there other points you would like to raise?

3000 character(s) maximum

There is an important role for international standards for compliance frameworks related to addressing illegal content, and we are advocating that the Commission explore including mechanisms in the DSA that support the development within the EU of such international standards. (We would note that online service providers successfully leverage an array of compliance frameworks for security, privacy, finance, trade etc.)

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

The maximum file size is 1 MB
Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

e53956d3-aa53-49d0-aea5-1978643efa08/Responsibility_Online.pdf

2 Other final comments

3000 character(s) maximum

A general note on some of the questions presented in this consultation: while we have endeavored to provide explanations and nuance under each of the scenarios and questions in the tables, we are concerned that this table format does not allow us to provide clear and accurate responses.

We would therefore stress the importance of the nuance we have provided under each table in the “please explain” questions that typically follow, and we remain at your disposal should you have any further questions.

Useful links

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

Background Documents

(BG) Речник на термините

(CS) Glosř

(DA) Ordliste

(DE) Glossar

(EL) ά

(EN) Glossary

(ES) Glosario

(ET) Snastik

(FI) Sanasto

(FR) Glossaire

(HR) Pojmovnik

(HU) Glosszrium

(IT) Glossario

(LT) Žodynėlis

(LV) Glosārijs

(MT) Glossarju

(NL) Verklarende woordenlijst

(PL) Słowniczek

(PT) Glossrio

(RO) Glosar

(SK) Slovnk

(SL) Glosar

(SV) Ordlista

Contact

CNECT-consultation-DSA@ec.europa.eu