Contribution ID: 04d32a4f-a332-4972-b1bc-c5c6c21ddb15
Date: 08/09/2020 17:41:03

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.

T h i s c o n s u l t a t i o n

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

Marie Anne

* 4 Surname

Nietan

* 5 Email (this won't be published)

M.Nietan@bitkom.org

* 7 Organisation name

255 character(s) maximum

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Federal Association for Information Technology, Telecommunications and New Media) (Bitkom)

* 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

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.

5351830264-31

* 21 Country of origin

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

( ) Afghanistan	( ) Djibouti	( ) Libya	( ) Saint Martin
( ) Åland Islands	( ) Dominica	( ) Liechtenstein	( ) Saint Pierre and Miquelon
( ) Albania	( ) Dominican Republic	( ) Lithuania	( ) Saint Vincent and the Grenadines
( ) Algeria	( ) Ecuador	( ) Luxembourg	( ) Samoa
( ) American Samoa	( ) Egypt	( ) Macau	( ) San Marino
( ) Andorra	( ) El Salvador	( ) Madagascar	( ) São Tomé and Príncipe
( ) Angola	( ) Equatorial Guinea	( ) Malawi	( ) Saudi Arabia
( ) Anguilla	( ) Eritrea	( ) Malaysia	( ) Senegal
( ) Antarctica	( ) Estonia	( ) Maldives	( ) Serbia
( ) Antigua and Barbuda	( ) Eswatini	( ) Mali	( ) Seychelles
( ) Argentina	( ) Ethiopia	( ) Malta	( ) Sierra Leone

- Armenia
- Aruba
- Australia
- Austria
- 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
- Falkland Islands
- Faroe Islands
- Fiji
- Finland
- 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
- Marshall Islands
- Martinique
- Mauritania
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar /Burma
- Namibia
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Singapore
- Sint Maarten
- Slovakia
- Slovenia
- 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

- Brunei
- Bulgaria
- Burkina Faso
- 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
- Haiti
- Heard Island and McDonald Islands
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Nigeria
- Niue
- Norfolk Island
- 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
- Timor-Leste
- Togo
- Tokelau
- 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

- Cuba
- Curaçao
- Cyprus
- Czechia
- Democratic Republic of the Congo
- Denmark
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- Lesotho
- Liberia
- Russia
- Rwanda
- Saint Barthélemy
- Saint Helena Ascension and Tristan da Cunha
- Saint Kitts and Nevis
- Saint Lucia
- Wallis and Futuna
- Western Sahara
- 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

Of course we do see the problem of illegal goods and content that can be found online. It is a reality that needs to be tackled. In the past 20 years since the emergence of the e-commerce Directive, the significance of information society services for society and economy has increased massively – bringing with it opportunities as well as risks and sometimes creating new policy challenges.

Rights holders/brands within Bitkom membership have experienced the case of fraudsters using the services of platforms to perpetrate frauds by misrepresenting themselves as the rights holder. Such frauds including phishing attempts. Further, rights holder regularly see imposter social media accounts created which can misrepresent the rights holder and/or redirect an end user to a commercial website where the user may be defrauded.

Rights holders/brands within Bitkom membership have in-house teams or external agencies responsible to identify fake listings and for making periodic test purchases for the purpose of reporting to the platforms or law enforcement authorities. Rights holders/brands within Bitkom membership bear considerable costs for

reporting to platforms the sale and offering for sale of counterfeit goods, other illicit products, false advertising, imposter accounts and the like. The means vary according to the company.

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

Actions following a report vary significantly between platforms in terms of transparency, efficiency and speed of reply. The documentation accepted to justify the notice also varies according to the platforms' respective processes.

It can happen that sellers immediately re-list the same illegal and illicit products, in breach of their contractual obligations with the platform, and therefore rights holders have to repeat the notification process which can be time consuming.

Many platforms also offer proprietary brand protection programmes that vary widely in scope, procedures, timelines and result. Bilateral contacts and relationships also exist.

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

Platforms cooperated even more closely than usual with the European Commission and other market authorities in tackling illegal goods online since the start of the Covid-19 outbreak. However, it is important to note that this cooperation and also the speedy removal of illegal goods in this situation of crisis was based on the existing notice and takedown mechanisms the platforms already had in place.

Platforms barred a great amount of products from its marketplaces that had inaccurately claimed to cure or defend against the coronavirus. Platforms also removed offerings from third party sellers who attempted to profit from the outbreak based on price-gourging.

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

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

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

21 Do you consider these measures appropriate?

Yes

- No
- I don't know

22 Please explain.

3000 character(s) maximum

B. Transparency

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

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

3 Please explain.

3000 character(s) maximum

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

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

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

3000 character(s) maximum

It is in the online platforms’ best interest to make sure that the user obtains information on why content is recommended to them, which is why most platforms offer such information already. Making the platform and user experience transparent and comprehensible is key to gaining the user’s trust.

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

The existing system of co- and self-regulation in Germany has proven to be successful. International cooperations of businesses, NGOs and public entities are able to ensure compliance with consumer and minors' protection standards in an effective and practicable way. In the long run, the system for protection of minors in a digital media world should increasingly rely on international models. The approaches adopted by the sector appear promising in this regard.

The concrete implementation of the protection mechanisms chosen by service providers lead to an effective protection of children from content harmful to them. It is essential to ensure that the user trusts that the service providers will recognise their possible share in the realization of the protection of minors on their services.

On EU level, better coordination of the interaction between the different age classification systems and the various self-regulatory bodies in the Member States would be helpful.

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

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

Social network providers and messenger services are active in two ways to combat fake news around COVID-19: if, on the one hand, users or authorities have reported misleading contributions, these are checked: either by external fact-checkers working on behalf of the social networks or by several checking teams of the social networks themselves. Contributions that have been proven false and misleading are made less visible or even deleted, depending on the potential risk. In addition, misleading advertisements that are intended to cause panic or suggest that advertised products, for example, are a cure or prevent infection, are also deleted. On the other hand, the operators of social networks counter fake news with easily found, reliable information. To this end, they cooperate with the German Federal Ministry of Health (BMG), the Federal Centre for Health Education or the World Health Organization (WHO), for example, so that they can place and disseminate their information on the platform in the best possible and most prominent way (e. g. on the homepage). For this purpose, comprehensive information centers with references to the WHO and the BMG are also prepared. In addition, there are some interfaces for messenger services. This means that you can chat with the BMG on important questions directly from the Messenger service. In particular, users searching for information on the Corona virus in social networks can access reliable sources in just a few clicks.

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

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

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)?

- [x]

A notice-and-action system for users to report illegal activities

- [x] A dedicated channel through which authorities report illegal activities
- [x] Cooperation with trusted organisations who report illegal activities, following a fast-track assessment of the notification
- [x] A system for the identification of professional users ('know your customer')
- [x] A system for penalising users who are repeat offenders
- [x] A system for informing consumers that they have purchased an illegal good, once you become aware of this
- [x] Multi-lingual moderation teams
- [x] 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

Many service providers invest heavily in systems for addressing illegal activities conducted by users. However, not all service providers carry the same risk-profile due to the nature of the service they offer. We therefore believe that any future framework should be sufficiently flexible and principles-based to allow providers to react in a way that suits their service best.

3 What issues have you encountered in operating these systems?

5000 character(s) maximum

Examples of issues that members reported are:

Erroneous, abusive and insufficient notices about allegedly illegal content, inlcuding blanket notices which lack substantiation or other data that would allow the service provider to identify the specific content and to determine its illegality;

Activities from bad actors who attempt to circumvent filters and other measures;

Limitations of automated systems to accurately detect potentially illegal content;

Lack of cooperation from public authorities, insufficient technological capabilities and understanding of authorities, inadequate of access to public resources;

Lack of legal expertise or lack of factual knowledge to accurately determine and assess illegality of content;

In many cases the determination of the illegality of such activity depends on circumstances that exist outside of the specific platform.

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

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

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

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

3000 character(s) maximum

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

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

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

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

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

Sometimes requests providers receive to share personal data appear at odds with EU data protection law: requests from law enforcement to share data on individuals without clear justification for the request, demands from authorities to share data absent a proper legal basis, and obligations to collect and share personal data which does not relate to the service providers business nor to the stated purpose of the original request.

There need to be guardrails in place regarding the kinds of data that can be requested from platforms, by whom, and for what purpose. Any subsequent discussion on whether to introduce obligatory data-sharing requirements for platforms in the framework of the Digital Services Act should bear in mind the specific nature of the various platforms, and the legal obligations that exist both for platforms but also for national and local authorities in terms of how to collect, treat and share personal data under GDPR.

The following questions are open for all respondents.

2. Clarifying responsibilities for online platforms and other digital services

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

	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)	Yes, only by larger online platforms	Yes, only platforms at particular risk of exposure to illegal activities by their users	Such measures should not be required by law
Maintain an effective 'notice and action' system for reporting illegal goods or content	◉	○	○	○
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

Since the DSA addresses a broad range of service providers and content, there needs to be a broad range of measures service providers can use in order to comply with the new legislation. This is why we propose a model close to that of the Audiovisual Media Services Directive, which lists several measures among which the service providers (in that case Video Sharing Services) can choose the most appropriate for their platform to prevent illegal content on the platform.

It is unclear, how ‘platforms at particular risk of exposure to illegal activities by their users’ would be defined, how this would be measured and finally decided on by whom. Therefore, we have doubts as to whether this classification is helpful in deciding over measures to legally enforce on platforms.
Linking regulation to certain thresholds (“larger platform”) or specific risks reflects a notion of proportionality – the idea that small enterprises should not be burdened with the same obligations as their larger counterparts which have more resources – and the circumstance that services with a high user volume have a greater societal and economic relevance. Even if this notion of proportionality is basically right, it is often difficult and sometimes also not generally appropriate to link regulation to specific threshold values, e.g. because of the nature of the market. Threshold values, a strictly quantitative approach, always go hand in

hand with a danger of legal inaccuracy and circumvention. In addition, depending on the framing of the provision, the result may be distortions of competition if competitors face different degrees of regulatory intervention. In the case of many provisions, a blanket limitation to large market players is certainly inappropriate, e.g. for notice-and-take-down. It would run counter to the objective of removing illegal content if only large undertakings had to comply with such a provision.

Content moderation teams should refer to content moderation teams for illegal content only.

Law enforcement agencies have legitimate interests in obtaining digital evidence to protect public safety and we support initiatives that make this process simpler while maintaining procedural safeguards. The European Commission's proposal for an electronic evidence regulation, if passed, would enable government authorities to obtain digital evidence from service providers, streamlining and harmonizing the process without sacrificing privacy safeguards. We remain concerned about proposals that would circumvent existing legal protections or require internet service providers to disclose user data to the government without any prior oversight by an independent authority and without proper safeguards. Such proposals would improperly shift the function of law enforcement investigation from government to private actors.

While the trusted flagger system is helpful, notices from trusted flaggers are not necessarily always 'better' than notices from regular users and should not categorically preferred over those. However, cooperation with 'trusted corporates' should be encouraged, i.e. sophisticated rights holders that have IP departments in place responsible for checking for and taking actions with respect to IP infringements.

Automatic detection is an important tool in tackling illegal content. However, those tools are not 100% reliable and their effectiveness depends on the platform and content in question. Therefore, their use should not be required by law. In specific cases in which those systems work rather well, e.g. copyright, they are already addressed in separate, more specific legislation.

Most marketplaces already inform their professional users about their legal obligations. However, one should keep in mind that it is not always possible to inform the specific user about every requirement under every national legislation that might possibly be relevant.

We recognize the desire for greater transparency around business customers on platforms. Such requirements should be reasonable and proportionate. Specifically, there should be a definition or at least guidelines on EU level on what constitutes a business user. We would therefore refer to the specifications on the 'Know Your Business Customer' principle in Compromise Amendment 4 of the draft IMCO report which specifies that this obligation should be 'limited to the direkt commercial relationships of the hosting provider'. We note the proposed "SHOP SAFE Act" in the US which proposes a seller vetting process that would require online platforms to take a series of measures. This may bring additional considerations for the EU discussion.

While the marketplace platform should inform consumers when they become aware of sale of illegal goods, informing consumers about recalls is the responsibility of the seller.

Cooperation with other online platforms is often mutually beneficial and should be encouraged but not made legally mandatory.

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?

- [x] Precise location: e.g. URL
- [x] Precise reason why the activity is considered illegal
- [x] Description of the activity
- [x] 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

For the notice-and-take-down procedure, EU-wide standards are needed as to what conditions a communication must meet in order to be valid, as well as what is necessary to prevent inadmissible communications, errors and abuse. For all legal remedy and anti-abuse mechanisms, information is decisive for identification. The more specific the conditions for a communication, the better, more seamless and rapid the processing operation and reaction.

Clarifying the concept of actual knowledge by introducing minimum requirements could be useful. A platform only has actual knowledge of illegal content if it receives a court order or is aware of the illegality due to a previous legal dispute or if the illegality is blatantly obvious, meaning that based on the information received, a customer support representative would be able to assess if the content is illegal without consulting a lawyer and would be able to make an accurate assessment as to appropriate action to be taken by the platform. Given that the fast removal of illegal material is often essential in order to limit wider dissemination, the receiver of the notice should have a clear policy available for handling notices, so that notifiers have confidence that notices will be considered and acted upon swiftly. Such notification systems should be accessible to all actors and easy to use.

Unfortunately, there can also be abusive recourse to the notice-and-take-down procedure posing a business threat. This must be taken into account, e.g. through explicit provisions on how to deal with (repeated) abusive communications.

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

Once several notifications have been received and accepted, and/or repeat offenders have been identified by the platforms' internal measures, the provision of services to that seller and its related accounts should be terminated because the terms and conditions of the platform have been breached. The platform should aim to identify its aliases/connected accounts – unfortunately, this is not always possible.

However, given the state of technology, over-reliance on automation presents a real risk of blocking lawful content and impacting the fundamental rights of European citizens. We therefore believe that notice and

takedown must remain the core standard. The prohibition on general monitoring obligations in Article 15 of the e-Commerce Directive should remain in place.

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

The opportunities and risks of automated tools vary significantly between different types of platforms and content.

Considering the vast amount of content that is uploaded, especially on bigger platforms, automated tools can present an important if not the only opportunity to deal with illegal and harmful content.

Especially with regard to audiovisual content (photos, videos) the automatic recognition of content already works very well in many areas, increasingly also with written utterances - whereby an automatic recognition of content does not necessarily lead to an automatic removal but first of all to a human verification.

It is important to keep in mind that automated tools, in contrast to human verification, are not capable of considering the context of pieces of content, which poses the risk of detecting content that, considering its context, is not illegal. Deciding whether a content is illegal often requires a high degree of interpretation. The circumstances of the statement, the tone of voice, the course of the discussion, the context, the question of including politically controversial topics, all this and more must be taken into account in the weighing process. Also exaggeration, exaggeration and polemics and even more so satire are covered by freedom of expression or artistic freedom. Those factors cannot be taken into account by automated tools which is why human oversight is still a very important factor in detecting illegal content.

Probably the majority of rights holders/brands within Bitkom membership have an open distribution model. If a trader uses a gallery image of a genuine product, it is difficult to determine if a product is illicit or fake from the ad/link itself. It is therefore difficult to see how an automated tool could determine if a product, the subject of the listing, is genuine or fake.

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

b.

When third country traders sell dubious products in the EU market, that are fake or breach EU health and safety requirements, this is problematic as they put the safety of European citizens at stake and reduce trust in the online economy.

Third country distributors must also comply with the legal framework, social and environmental standards applicable in the EU and ensure that their products are not dangerous to consumers and do not infringe intellectual property rights. Consumer protection and a level playing field are essential. It must also be ensured that German or European rules can be enforced equally with traders and platforms from third countries as with those from the EU.

The aim must be that traders and platforms, regardless of where the company is based, comply with the law when they sell to European consumers.

Irrespective of whether traders from third countries make use of services from European fulfilment service providers for the storage and dispatch of their goods, the goods must be cleared by customs when imported from third countries. However, customs authorities are often unable to verify products due to heavy workload as well as lack of resources, training and expertise.

The Commission, together with intermediaries, other stakeholders and customs authorities should explore what measures can be taken to ensure that products sold online in the EU market are genuine and meet the relevant EU health and safety regulations. Such measures should be workable and proportionate.

In our opinion, customs authorities' capacities should be increased for this purpose. Digital registration with customs and the promotion of the European one-stop shop would also be useful measures. Novel and intelligent technologies should be used to improve and expand the capacity of law enforcement authorities to identify and stop counterfeit and pirated goods and to reduce the number of 'bad' traders.

Furthermore, there is a need to improve the "notice-and-take down" procedure by which offers can be removed from the platform after the authorities, consumer associations or trademark or IP owners have been informed of any infringement of the offer, the product's origin, the indication (and where appropriate, verification) of the manufacturer's seat.

Once a rough seller has been identified by an intermediary there should be an information flow between the intermediary and customs authorities to improve crime detection and seizure at the border which would protect EU consumers from any dangerous or counterfeit goods purchased online.

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

A horizontal and yet differentiated approach is necessary which takes into account the different technical architecture of services and hence a particular provider's de facto insight into and possibilities for dealing with illegal content. For instance, Internet access providers have neither knowledge about nor control over information transmitted via their communication network, not least because this is forbidden by regulation on network neutrality.

It is appropriate in some circumstances to supplement or subdivide the existing provider categories under eCD (host provider, access provider, caching provider) with further categories and specific rules, still taking the technical architecture of service providers into account. For example, cloud services tend to act passively and usually have neither knowledge about nor control over content stored on their platform. Given their

technical architecture designed with privacy protections and their contractual relations they hold towards their customers' data, these services are more restricted in their possibilities to combat illegal content uploaded by their users. Expecting such passive services to make efforts to manage content comparable to those required of publicly accessible services for shared use of content is not only technically infeasible, it runs counter to their technical and operational character and would lead to unjustified data protection, security and commercial overlaps. Thus, whether or not a service allows the sharing of content with the public could also be adduced as a criterion for an overlap between services.

Similarly, what makes sense for content-sharing platforms may not be appropriate, or technically feasible, for a search engine, or a platform that hosts mobile apps. Regulation must also ensure respect for user privacy, where users communicate privately or in small groups, and where they use anonymization or pseudonymization.

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

Tackling illegal activities online cannot be done by one part of society alone: Actors from the economic and political realm as well as general society need to exchange knowledge, experiences and best practices and be ready to face the problem together.

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

Content (in particular user-generated content) on platforms which is classified as "legal but harmful", e.g. false intelligence, can often be addressed better through self-regulation than through strict regulatory requirements. This is a more efficient instrument in this area, since constantly changing harmful content can be better taken into account through greater flexibility and more rapid adjustment. But first and foremost, the necessary legal framework for dealing with this type of content is completely different from that for illegal content, and there is a stronger link to restriction of personal rights. It is often very difficult to evaluate whether or not user-generated content is illegal. Whether content is "harmful" is often less easy to decide on the basis of clearly defined criteria, since this depends even more strongly on the relevant context/user group. Content that is appropriate on some sites may be inappropriate on others; what may be appropriate for some users may be inappropriate for others. Rather than dictating content policies, regulation could require that services come up with appropriate guidelines and safeguards.

Provisions on harmful content should not be covered by the digital services act. Nevertheless, it must continue to be possible for providers to moderate harmful or otherwise unwanted content in their service in line with their own (transparent) rules.

Any future framework should be sufficiently flexible and principles-based to allow service providers to react appropriately to the concerns that are specific to their services and reasonable with regards to their unique situations and abilities. For example, online marketplaces which connect buyers and sellers raise fundamentally different regulatory issues to social media platforms, and the risk of harm to users varies accordingly.

The focus on illegal content and activity in the updated liability framework need not preclude further evaluation and action on “lawful but harmful” content through self- and co-regulatory initiatives, which have proven success through EU initiatives such as the Code of Conduct on Hate Speech and the EU Code of Practice on Disinformation.

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

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

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

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

It is vital that regulation protect citizens' fundamental rights. Article 19 of the Universal Declaration of Human Rights makes free expression a human right. Standing up for free expression means enabling access to content, including content that some people may find offensive, frivolous, or controversial.

We remain concerned about regulation that would restrict the ability of services to maintain diligence in assessing content, and in particular the risks to fundamental rights where companies are forced to prioritize speed of removal over careful decision-making.

The Council of Europe's Committee of Ministers recommendations on the roles and responsibilities of internet intermediaries also included a set of guidelines for States. They recommend that:
State authorities should obtain an order by a judicial authority or other independent administrative authority, whose decisions are subject to judicial review, when demanding intermediaries to restrict access to content;
States should make available, publicly and in a regular manner, comprehensive information on the number, nature and legal basis of content restrictions or disclosures of personal data that they have applied in a certain period through requests addressed to intermediaries.
The Committee also cautioned that disproportionate sanctions would likely lead to the restriction of lawful content and to have a chilling effect on the right to freedom of expression

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

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, reports on companies' policies and measures on illegal content and goods are a useful tool to enhance transparency and traceability of their actions. Therefore , many companies already publish reports that provide information on how much content has been reported and, if necessary, removed, also through automated systems. However, the methods used may vary from company to company, so the reports will not necessarily be comparable. In any case, the functioning of these procedures can only be described to the extent that business secrets are not affected and not enable bad actors to circumvent the systems that are in place.

It will be important to clarify exactly what should be part of those reports and for which purpose these information will be used by regulators or authorities. When defining the content of these reports it is important to take into account what is technically and administratively feasible/proportionate for the companies and also which transparency obligations from other regulatory pieces exist already.

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

Proportionate requirements of basic transparency on automated systems towards customers can be a useful tool but should not entail disclosure of details that overstrain customers or that amount to business secrets. Consistency has to be ensured with transparency rules in other regulatory acts.

Users should be given a general understanding of how the algorithm works to help them find content that is relevant to them. However, it is important to understand that disclosing the underlying algorithms could open up such systems for abuse and risks to trade secrets.

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

5000 character(s) maximum

With an eye to possible new transparency rules for the ranking in Internet service offers, it is important to understand that this is influenced by a range of factors and filters. Moreover, any transparency obligation should comprise protective measures against passing on business secrets. Under no circumstances should consideration be given to general provisions which make disclosure of concrete algorithms obligatory, since in many cases they constitute a core element of a provider's business model. Revelation of too much information about the functioning of algorithms can also lead to them being compromised by fraudulent

players (hackers, spammers, etc.), which can ultimately harm the consumer. Rather, the publication of generic and general information should be required at most. This is already clarified in the relevant provisions of the modernisation directive and in the P2B regulation.

Binding rules on ranking need to take into account all relevant existing provisions, prevent potentially negative impact on trade secrets and mitigate possible risks such as opening up processes to manipulation. Transparency is an important facilitator of trust which is why many platforms already provide transparent information as envisaged by the proposal. Whatever their size, online intermediaries have a strong interest in both the success of their business users and the consumers' trust. This is why they have set up tools, analytics, APIs and information to support their business users and rules to ensure that the content, services or goods provided on the platforms are safe and secure for the consumer. Both, tools and rules, are used by platforms to compete with each other, either to differentiate their content, services and goods from others' to attract and retain consumers, or to create the best support to attract business users. Any regulation must be fully aware of this self-regulatory framework and the fact that platforms have to balance the interests of business users and consumers. However, where such measures are not implemented and issues regarding transparency arise, provisions can facilitate an improvement in fair competition and trust between the contractual parties. Nevertheless, it is important to understand that the ranking on an online intermediation service site is influenced by a variety of factors and filters. Some of these are completely out of the scope of the provider´s control, e.g. if a user decides to sort by price, location, specific technical features, etc. Such options are commonly known, so there is no practical need to regulate them.

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

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

It might be appropriate to supplement or subdivide the existing provider categories under the Directive (host provider, access provider, caching provider) with further categories and specific rules, still taking the technical architecture of service providers into account. Especially the category of 'hosting service providers' is very broad. Were the Digital Services Act to propose responsibilities for those providers, a more differentiated approach would be necessary. For example, cloud services tend to act passively and usually have neither knowledge about nor control over content stored on their platform. Given their technical architecture and their contractual relations with users, these services are therefore more restricted in their possibilities to combat illegal content uploaded by their users. Expecting such passive services to make

efforts to manage content comparable to those required from publicly accessible services for shared use of content runs counter to their technical and operational character and the relationship with users, and would lead to unjustified data protection, security and commercial overlaps and legal friction. Thus, whether or not a service allows the sharing of content with the public could also be adduced as a criterion for an overlap between services.

A harmonized, graduated and conditional exemption scheme continues to be needed as a foundational principle of the internet. We understand the need to ensure the framework reflects the nature of today's services.

Concerning specific categories of service providers:
Digital infrastructure services would still be required to meet equivalent conditions to the existing Article 12 to benefit from the liability exemptions.
Cloud providers are limited in what they can do to address illegal content stored by their customers or by their customers' users, or respective activities undertaken, given the technical architecture of their services designed with privacy protections and the contractual obligations (particularly confidentiality and abstention from accessing stored information) they hold towards their customers' data. We believe cloud providers, including software as a service ("SaaS") providers, should fall into a separate category of service, similar to the current category of caching services. This would reflect the reality that factually and contractually, such providers do not have the required authority and control over content such that they should have responsibility for removing specific content from a third party's service. Where a third party digital service provider uses a cloud provider, that third party should remain responsible for compliance with the law.

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

The Digital Services Act is an opportunity to clarify the 'knowledge standard' taking into account the jurisprudence of the Court of Justice of the European Union (CJEU). A distinction should be made between mere passive hosting providers and those that are actively involved in the distribution of goods (storage, labelling, shipping, payment acceptance) such as online marketplaces. Descriptions such as "current level of knowledge" and "degree of control" may be helpful in making the distinction. A platform only has actual knowledge of illegal content if it receives a court order or is aware of the illegality due to a previous legal dispute or if the illegality is blatantly obvious, meaning that based on the information received, a customer support representative would be able to assess if the content is illegal without consulting a lawyer and would be able to make an accurate assessment as to appropriate action to be taken by the platform. Given that the fast removal of illegal material is often essential in order to limit wider dissemination, the receiver of the notice should have a clear policy available for handling notices so that notifiers have confidence that notices will be considered and acted upon swiftly. Such notification systems should be accessible to all actors and easy to use.

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

Hosting providers in particular should be encouraged to take proactive voluntary measures to remove illegal content from their platforms. However, any such efforts undertaken by providers must not affect the continued existence of the liability privilege. Proactive measures can indeed lead to the provider acquiring knowledge about illegal content. However, the hosting provider has the possibility in such cases to remove or block access to illegal content as soon as it has acquired knowledge about it. If the hosting provider does this, it continues to enjoy exemption from liability. This is in line with the European Commission's 2017 communication on tackling illegal content online (pages 10-12).

It should also be made clear that proactive measures do not lead to the provider automatically having knowledge about all the content it stores. It is therefore important to create legal certainty about the standard of knowledge required in the framework of the liability protection regime. In this context, the following should be clarified:
a) if a service provider voluntarily checks some content in order to ensure that it does not infringe one or more laws, it is assumed that this provider does not have any knowledge about the illegality of other content on its platform which it has not checked for such purposes; and
b) if a service provider voluntarily checks content in order to remove content which infringes a particular law, it is assumed that this provider does not have any knowledge about all other possible legal infringements which could be committed by the same content but which were not part of the check.

Without this clarity, the risk that a service provider - taking proactive measures in good faith - will be assumed to have knowledge about all content of its services, could act as a deterrent to taking such responsible steps. Furthermore, thought could also be given to provisions which provide for a positive incentive to introduce such voluntary measures – e.g. through a facilitated distribution of the burden of proof for the providers in question.

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

In some cases the concept still today is sufficiently clear and remains valid; in other cases, the applicable threshold to delineate 'active' from 'passive' has become unclear. The distinction in some case law between "active" and "passive" hosts particularly creates significant uncertainty and liability risks for common features of current services. There is no clear view in Member States' court rulings of what this distinction means and which services are, or are not, "active". Further, to relate "active" status, as some courts have done, to the notion of algorithmically "optimizing" content is acknowledged as being outdated in light of today's services. The recent Advocate General Opinion in joined cases Peterson vs. YouTube (C-682/18) and Elsevier vs. Cyando (C-683/18) highlights that "Optimising access to the content should not, in particular, be confused with optimising the content itself." (Para 83).

In addition, and as discussed above, an intermediary that engages in voluntary moderation risks being labelled as an "active" service provider, or otherwise being deemed to have knowledge of all of the content on its platform.

We believe the Digital Services Act should move away from the unclear concept of "active" hosts, and replace it with more appropriate and differentiated concepts reflecting the technical reality of today's services, building instead on notions such as actual knowledge and the degree of control.

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 ban on imposing a general obligation to monitor, established for all information society services (article 15 eCD), should be maintained, since this constitutes a further fundamental building block of Internet regulation and is an important condition for the creation and development of platforms and further services. Without this ban, the Internet economy would probably not have been able to develop into what we see today, and service providers would face considerable challenges, which would – in many cases – make the development of new services, platforms and business models substantially more difficult. Any such prophylactic, blanket and all-encompassing monitoring obligation would not be apt to provide for a solution in respect of the complex challenges generated by illegal content; it would pose enormous risks for collateral damage. We are heartened by the Commission's promises to maintain the ban on a "general obligation to monitor".

It is also important that this ban is not totally deprived of all its effects by having recourse to the imposition of "monitoring obligations in a specific case" excluded from the ban as set out in Article 15 eCD (cf. recital 47). Relevant rulings by the European Court of Justice make it clear that a specific monitoring obligation only encompasses cases which do not entail monitoring of all up-loaded content aimed at assessing possible legal infringements for an unlimited period of time.

Any voluntary measures clause that may be considered under possible options should be very clearly defined as to its scope and limits.

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

We broadly welcome the idea that the horizontal regulatory approach of the e-commerce directive which covers each and every information society service is to be further developed. It is important to pre-serve the central, fundamental, generally valid and hence horizontally applicable principles of the directive such as the conditioned liability privilege, the ban on a general monitoring obligation and the country-of-origin principle.

However, beyond this, it is important to bear in mind that these services are characterised by highly varied business models and that there can be no "one-size-fits-all" solution for dealing with illegal content over and above the generally applicable principles. Accordingly, these differences must not get out of sight when assigning rights and obligations and in particular when it comes to defining the acceptability of measures that should be taken by providers.

Intermediary digital service providers from a very wide range of sectors are covered within the category of hosting provider – from social networks and suppliers of short-term lets to online marketplaces. Furthermore, the focus is on a large number of different types of content – from audiovisual media or user-generated content, holiday-home offers to the offer of physical goods. A differentiated approach, as mentioned above, should also take into account the different types of content and possible measures for dealing with these

content types. The specific risk potential is also central for the differentiation (in treatment) of different kinds of (illegal) content.

Within the existing regime, an improvement to and harmonization of the notice-and-take-down procedure at European level is necessary where deficits have been identified. Such procedure must comprise a solid guarantee of fundamental rights and eliminate current legal uncertainties. For the notice-and-take-down procedure, guidelines are needed as to what conditions a communication must meet in order to be valid, as well as what is necessary to prevent inadmissible communications, errors and abuse. For all legal remedy and anti-abuse mechanisms, information is decisive for identification. The more specific the conditions for a communication, the better, more seam-less and rapid the processing operation and the subsequent reaction.

In addition, there could be uniform provision for what is to be done in a disputed case of a take-down. In this regard, it is important to bear in mind and recognise that, because they offer different services and content, different providers face different challenges which can be met in different ways through notice-and-take-down. In other words, providers also have different expectations of a notice-and-take-down procedure. In any event, notice-and-take-down procedures must take into account the specific features of individual sectors, always be oriented around the principle of proportionality and be structured differently where necessary. Alternatively, it could be explored to foresee a counternotice procedure in line with the DMCA provisions. Unfortunately, there can also be abusive recourse to notice-and-take-down procedures posing a business threat. This must be taken into account, e.g. through explicit provisions on how to deal with (repeated) abusive communications.

The distinction between taking on voluntary responsibility and legal liability is important. While maintaining the general liability privilege, possibilities for taking on responsibility as a function of the type of service provider and content should be discussed.

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?

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree	I don't know/ No reply
Consumers have sufficient choices and alternatives to the offerings from online platforms.	○	○	◉	○	○	○
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

A well evidenced and holistic assessment of the market activities should constitute a key criterion.

Online platform services are diverse and cover different services, markets and activities. Quantitative thresholds based on turnover, user numbers or geographic scope seem arbitrary and alone should not constitute a “gatekeeping” role of a company. It is therefore our view that qualitative criteria appear to be better to assess a potential gatekeeper position.

All the criteria should also be clear and predictable to ensure legal certainty. We are of the strong opinion that the criteria should always be combined as only one or few criteria would not be enough to define a gatekeeping role.

The currently discussed wide geographic coverage in the EU criterion appears ill suited to identify gatekeeper platforms. Market conditions that can lead to such a position can exist across a small number of even only one single member state with the same potential risks for business users and competition. If the goal of the regulation is to protect contestability of markets and protect business users then this should apply anywhere where there are concerns.

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

The question seems to combine different aspects and is therefore not suited to answer the question whether certain activties could strengthen a gatekeeper role. The listed options will therefore not bring clarity to the gatekeeper role/definition.

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

We believe that enabling growth, innovation and the success for digital companies in Europe a favourable investment framework is key. One of the most important factors should be a strong entrepreneurial foundation and a harmonized single market. Factors such as support for entrepreneurs, innovation hubs, regulatory sandboxes, skills and education, as well as access to a range of different funding solutions, all play a role in encouraging start-ups and promoting their success.

Startups and scale-ups naturally will depend on larger companies, some of which are platforms while others are not. The small vs big business situation is not unique to online-driven markets and similar situations exist in the offline world where e.g. retailers decide on the fate of products by listing or de-listing them or where large investors essentially chose who to invest in. The current debate unfortunately neglects the fact that platforms, no matter whether they are gatekeepers or ordinary platforms, on bringing together various types of business and consumers and therefore have a natural interest in seeing them succeed. Multi-sided

markets above all mean there is a multi-sided dependency as well as symbiosis between all players.

Some markets / ecosystems are characterized by digital gatekeepers that can hardly or not at all be contested. In these cases, a level playing field, fair and effective competition constitute the necessary condition for smaller rivals and potential entrants to succeed. It is not a sufficient condition for market success, expansion, etc., but a neccessary one that needs to be ensured.

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

Platforms have enabled especially small businesses to reach consumers across the single market, significantly reducing existing barriers and driving innovation. They also allow citizens to share and consume information across various offers and shop across borders on trusted, safe and predictable environments. The policies that platforms set for their services need to strike a careful balance of all interests involved – freedom of expression or a business user's freedom to offer products and services on the one side and societal and individual citizen interests on the other. At the same time, we are aware that there can be negative impacts and that this important task of balancing various interests will necessarily lead in some cases to unwanted effects, which should be tackled in targeted manner.

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

New, dedicated rules would only be justified where there are disproportionate risks specific to certain service providers under clearly pre-defined conditions.

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

Whether there is need for a specific regulatory authority cannot be answered without clarity on new regulatory powers and tools. But any enforcement system should provide for sound evidence based decision making, comprising all faire hearing rights, due process and full rights of appeal to a higher court.

The enforcement mechanism should be at EU level to ensure coherence and harmonization in the single market and avoid potential inconsistencies in application across member states. It should in any case ensure legal certainty and a level playing field across the EU. Incoherent enforcement could negatively impact competition and pose significant hurdles for the Internal Market.

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

While we have no particular view on the potential enforcement setup, it should in any case ensure legal certainty and a level playing field across the EU. Incoherent enforcement could negatively impact competition and pose significant hurdles for the Internal Market. If such rules were to be adopted, an existing body with the required level of experience should be in charge of enforcement.

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

Given both prohibitions and obligations as well as case by case remedies will likely be intertwined and may even impacts on each other as well as the overall business strategy for covered companies, the same authority should be in charge of them in order to avoid inconsistent and uncoordinated enforcement. Furthermore, since most large online platforms are active in more than one member state, with business

users and consumers interacting across borders, remedies will in most cases have to be developed for the whole of the EU. Finally, in order to develop meaningful and proportionate remedies, the authority in charge will have to invest significantly in technical and market expertise, which may not be possible for smaller authorities.

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

Sector-specific rules should continue to apply and have precedence over any gatekeeper rules. Any obvious overlaps or conflicts should however be explicitly address in the gatekeeper regulation in order to avoid situations of legal uncertainty.

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

The rules could address both negative societal and economic effects, however this distinction may not always be clear. Importantly, some platforms may exhibit greater negative societal effects than others and any measures should therefore be carefully targeted at those concerned business models. At times, societal and economic goals may even conflict, which is why their interrelationship should be addressed in the same legal framework.

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

It remains unclear what is meant by “large amounts” and what “data” in practice. Data may be personal data or transaction data. It can be individual consumer or business user data or be aggregated. It can be raw or processed data or be combined with other existing data. Data is very rarely exclusive to specific companies given business users and consumers typically use several services that collect the same or comparable data. Furthermore, data plays a different role in zero-price markets with advertising-based business models compared to cases where services are offered against remuneration.

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:

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

20 If other, please specify

3000 character(s) maximum

The authority needs to build up significant expertise in digital-driven business models and markets to ensure any enforcement activities stimulate competition and innovation rather than stifling it.

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
- [x] Monitoring powers for the public authority (such as regular reporting)

- [x] Investigative powers for the public authority
- [x] Other

23 Other – please list

3000 character(s) maximum

Investigation and monitoring are the only appropriate mechanisms and there already exist well-tested investigative and monitoring systems (in e.g., comp law), which can be drawn upon.

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

The fair application of such rules should be carried out by an EU level enforcement body with investigative and monitoring powers.

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

In the consultation, the term “large online platforms acting as gatekeepers” is used to describe what is in fact a broad and heterogeneous collection of companies. EU comp. law is in place to address any conduct engaged in by market operators, incl. online services that may interfere with the proper functioning of a market. Other regulatory mechanisms are available to deal more specifically with other policy issues, such as consumer protection or data protection rules. Any regulation targeting structural features resulting in durably foreclosed or hardly contestable markets needs to be carefully balanced with existing competition law provision, evidence-based, problem-oriented and targeted, complementing existing regulations. Any initiatives should first await the impact of recently adopted P2B regulation and build on the respective evidence. The P2B sets new requirements for all online platforms no matter their size or market power, precisely recognizing that a natural differential in negotiation powers between platforms and business users bears risks. However, it explicitly limited intervention to targeted measures proportionate to the evidence of market failure. An aspect not reflected yet in the Consultation is that of judicial safeguards, procedural fairness and respect for rights of defence for companies in scope of a potential gatekeepers regulation. Speed of enforcement must not come at the cost of due process. Especially outright prohibitions of business practices have a significant risk of regulatory failure and require careful assessment of the effects on competition, innovation and consumer welfare. Finally, the relationship between the gatekeepers regulation and the NCT remains unclear. There is no need for two parallel initiatives, addressing the same companies, which would potentially be enforced by different authorities, raise the risk of fragmented and inconsistent decisions with the potential to disproportionately limit the freedom to do business. The development of any ex-ante regulatory instrument should focus on promoting user interests and benefits, innovation and appropriate regulation as technologies and markets evolve. The designation of companies as "gatekeepers" must be based on clear definitions and backed up by evidence; it cannot and must not lead to discrimination against particular business models or technologies.
The instrument of ex-ante regulation must take into account existing measures, initiatives and regulations; any gaps should be demonstrated before starting to examine potential solutions. It is important that all ex-ante rules for platforms are aligned with all other initiatives proposed by the Commission, including the proposed NCT and the revision of the Notice on market definition. We believe that we need to find targeted, proportionate approaches to solving specific problems, while avoiding blanket new bans and overlapping frameworks that would restrict economically and socially useful innovation.

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

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

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

Smart contracts are lines of code to facilitate the execution of specific elements of a transaction. They are not using artificial intelligence nor analytics software; neither do these replace “traditional” contracts (i.e. agreements written in plain terms).

Therefore, we do not currently perceive any difficulty, nor see a need for a regulatory framework related to smart contracts (neither, for instance, to (i) strengthen their enforceability; nor to (ii) contain mechanisms to halt their execution).

The rationale is that the contract documents (traditional contracts), use plain words and can and should therefore properly and sufficiently include such mechanisms. These classical contracts also guarantee the enforceability of the contract that describes the project or commercial transaction which involves the use of Blockchain technology (and hence the lines of codes used to support the execution of this commercial transaction).

These lines of codes (called “smart contracts”) should not replace traditional contracts entirely in the short term, they should rather support the automated performance/execution of certain elements of the transaction described in such traditional contracts.

As mentioned, smart contracts can be a tool, a simple peace of code. Like paper and pencil in the classical world, smart contracts are a tool to write something down in the digital world e.g. a certificate. The legal requirements of the certificate depend on the content of the certificate and not on the tool.
We need more regulatory requirements for the product and processes represented by the smart contract and the environment e.g. platforms in which smart contracts operate, not for the tool “smart contract” as such.

Smart legal contracts on the other hand can be part of legal/traditional contracts, representing the operational aspects in the lifecycle of a legal contract. One example is the verifiability of rental contracts. Once the bank verifies the signature of the tenant in the bank statement, the tenant can use the verified bank to sign the monthly rental payment. There is a monthly verification of the contract. In addition, including platforms, e.g. blockchain allows the enforceability of smart legal contracts.

We need legal clarity for smart legal contracts to use verification and enforceability to increase efficiency of processes.

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
- [x] Minimum standards for the validity of “smart contracts” in the EU
- [x] 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
- [x] Further clarity for payment and currency-related smart contracts.

4 Please explain.

3000 character(s) maximum

We want to emphasize that smart contracts are not limited to blockchain. New regulatory requirements need to make sure that this stays like this.
Smart legal contracts and smart contracts existed before blockchain platforms popularized them. Their application field is broad. Smart legal contracts e.g. have already been used successfully in court as evidence. The validity of smart contracts is not in the scope of EU regulation. It is the underlying process or the product represented by the smart contract that is or should be in the scope of EU regulation. What we need is clarity on standards and requirements, even when focusing on the verifiability guarantees and not only on the live systems where they could operate.
Further, it is important that we obtain a common understanding of who is liable, if different parties e.g. product owners, issuers and service providers are involved in a smart contract. One example are payments. We need requirements for the digital euro and the smart contract using it has to be designed accordingly. Moreover, we need legal clarity for the transfer of property rights e.g. signatures, stamps and digitization of paper requirements, to allow a technical implementation with smart contracts. Many of the current use cases revolve around the transfer of property in systems that guarantee the enforceability of these transactions. It would be helpful to clarify the space of use cases where the feasibility is not only technical but also legal.

5 Are there other points you would like to raise?

3000 character(s) maximum

All regulatory approaches on European level should keep in mind that the technology behind smart contracts, blockchain and DLT is global. If we guarantee a technology neutral, transparent and reasonable framework, Europe can play a decisive role in the digital space. A major step to make smart contracts suitable for the mass market and to enhance innovation further is a harmonized EU wide classification for crypto assets and a digital payment concept.

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

Different reporting obligations

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

Fragmentation around process rules presents practical challenges for platforms, 27 different sets of process rules might lead to unworkable systems. Practical challenges include the significant cross-organisational efforts in setting up each compliance framework, and the lack of standard definitions, metrics or methods in designing product solutions. These challenges also extend to transparency reporting – there are practical difficulties in preparing reports that have varying definitions, metrics and methodologies. Our preferred approach is to support the Country of Origin (COO) principle in the DSA and ensure harmonization of processes, with a longer term goal of developing international standards for compliance practices.

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

Improving legal enforcement is a central factor and is a complementary building block for the discussion on introduction of updated obligations. An important role is played here by measured, efficient supervision as well as enforcement of existing obligations. Better cooperation between national supervision authorities is also necessary here, and support is desirable in order to prevent divergent application and enforcement of provisions designed to be uniform across the EU and to ensure consistency.

Some digital platforms still struggle with significant regulatory fragmentation, despite the existence of Country of Origin principle. National and local governments who wish to enforce obligations against platforms as an exception to the Country of Origin principle often do not notify the Member State of Origin or the European Commission of their intentions, offering no opportunity for an assessment of the local rules in the context of EU laws, nor an ability to enter into dialogue to resolve those inconsistencies. All derogations from the Country of Origin principle must be exceptional, clearly aligned with EU legal frameworks and there has to be a clear process for notifying the Commission. Additionally, an enforcement process must be in

place for impermissible derogations. The DSA could therefore further clarify how the Country of Origin principle works in practice 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 an online platform.

Reverting to a Country of Destination principle would hamper growth opportunities for all businesses across the Union, with numerous unintended effects. Enabling Member States to immediately adopt desired exceptional measures (though the Commission shall be informed), or reverting to COD when the path forward is disputed or unclear, leaves no opportunity to enter into dialogue to resolve inconsistencies, and erodes the ability of the EU institutions to adequately assess measures and enforce the Single Market.

Nevertheless we call for maintaining the right of a party to seek redress in a dispute in accordance with Brussels I, other specific instruments such as the Trade Marks Regulation, and recent case law developments. Both the EU Regulation No.1215/2012, often referred to as “Brussels I” and Council Regulation (EC) No.207/2009 (“the Trade Mark Regulation”) contain exceptions that allow a party to choose either to sue a defendant in the country of origin or in the country of destination based on rules elaborated in case law such as the recent ECJ decision C-172/18 AMS Neve Ltd.

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

No matter which concrete form of governance will be chosen it is of utmost importance that competencies and responsibilities are clearly assigned between authorities making it easier for the service providers to know their 'go-to' points. It is also important that authorities are willing to enter into dialogue with the service providers to find constructive solutions to upcoming issues.

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

3000 character(s) maximum

Procedures, modus operandi, contact points

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

With regard to a possible EU-level authority for the supervision of platforms it is questionable whether and how it could be ensured that one authority disposes of the expertise to deal with all sorts of platforms from different sectors, with different business models and different types of content.

Nevertheless, a central authority could support cooperation between member states as well as between member states and platforms by sharing best practices and legal advise, underlining the Country of Origin principle. A key contribution could be to resolve situations to prevent lengthy court proceedings, which are currently the only means open to platforms and service providers to challenge the proportionality of local regulations.

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

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

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

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

2 Other final comments

3000 character(s) maximum

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