

# 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**



- 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

\* 4 Surname

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

\* 7 Organisation name

*255 character(s) maximum*

Austrian Federal Chamber of Labour

\* 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

16 Does your organisation play a role in:

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

17 Is your organisation a

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

18 Is your business established in the EU?

- Yes
- No

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

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czechia
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland

- Portugal
- Romania
- Slovak Republic
- Slovenia
- Spain
- Sweden

## 20 Transparency register number

*255 character(s) maximum*

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

2386947191154

## \*21 Country of origin

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

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

- 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
- Brunei
- Bulgaria
- 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
- Haiti
- Heard Island and McDonald Islands
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar /Burma
- Namibia
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Niue
- 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
- Timor-Leste
- Togo

- 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
- Cuba
- Curaçao
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- 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
- Russia
- Rwanda
- 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
- Wallis and Futuna
- Western Sahara



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

## \* 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

2 What measure did you take?

- I sent the product back to the seller
- I reported it to the platform via its existing reporting procedure
- I contacted the platform through other means
- I notified a public authority
- I notified a consumer organisation
- I did not take any action
- Other. Please specify in the text box below

3 Please specify.

*3000 character(s) maximum*

One of the tasks of the BAK is to advise consumers and support them in cases of conflict. In individual cases, contact is made with platforms or specialised NGOs (such as the Internet Ombudsman Association) are requested in their "trusted flagger" capacity to report legal violations to the platforms. Cooperation with individual platforms does not always work satisfactory in these individual cases. Above all, the high number and dynamics of fraudulent or otherwise illegal practices sets narrow limits on the chances of consumer protectionists to enforce law. Fraudulent offers are often ranked first in the Google Search results list. When searching for products via Google Picture, there are often more fake shops that target prepayment fraud than serious offers are displayed. Tests published by the BEUC consumer network (<https://www.beuc.eu/publications/twothirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html>) also show the enormous risk of consumers being offered online products that are dangerous to their health. Whether electrical appliances, toys or cosmetics: 66% of the products offered on platforms such as Amazon, AliExpress or eBay products examined did not comply with the EU minimum safety standards (risk of carbon monoxide poisoning, 200-times in excess of permissible chemical ingredients, fire hazard, etc.). Another test result: when dangerous products were removed from platforms after being reported, they immediately reappeared at new addresses. The platform providers do not generally consider themselves responsible for product safety issues and therefore check providers who are not particularly risk averse to such issues before they are activated, using criteria such as sensitive product groups, countries of origin without equivalent safety standards, recurring characteristics of already blocked providers, etc. Against this background, mere reporting systems without formulated platform obligations and liability are not a suitable way of enforcing law effectively. It is crucial to impose a "know your customer" obligation on platforms. Currently, the most popular trading platforms do not (sufficiently) check their commercial customers before they are activated. In comparison, local platform providers in Austria want to know much more about the seriousness of the commercial providers licensed on their platforms. On the other hand, consumers constantly come across companies on the dominant platforms that are not capable of taking legal action and do not provide addresses or falsified information, mere P.O. box addresses or exclusive headquarters in third countries such as China without representative offices within the EU.

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*

According to the feedback from consumers, they only receive an automated standard response after their reports, which does not respond to their specific submissions. This means that the platform thanks them for their report. Thus it remains unclear to consumers what happens after the notification. In the event that products or providers are actually blocked, the BAK has received reports from consumers that, shortly after this short-term success, exactly the same products with the same names and prices can be found online again. The whole process is constantly repeated, so that no final solution to the problem can be found. Finally, consumers stop reporting goods or suppliers because they are frustrated and find that their aid is not going to do anything substantial anyway.

## 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*

In our experience, consumers find illegal goods through a simple internet search or through social networks. They assume that the offers are checked and controlled by the suppliers. This leap of faith leads them to open a search result thoughtlessly and/or click on an advertisement without question and order the illegal goods. A remedy may be that advertising for certain suspicious product groups may only come from reputable traders. If consumers report an illegal product, the processing should not be limited to this specific report, but should include further tasks: Platforms are to investigate whether, in connection with the report, other products from the same supplier/registrar are conspicuous and equally suspicious. If the platforms discover anomalies, they are to block further offers that have not yet been reported or entire traders, irrespective of the specific report.

## 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

## 12 What measure did you take?

- I reported it to the platform via its existing reporting procedure
- I contacted the online platform by other means to report the illegal content
- I contacted a national authority
- I contacted a consumer organisation
- I did not take any action
- I took a different action. Please specify in the text box below

## 13 Please specify

*3000 character(s) maximum*

We refer to our information under point 3: The platforms do not always respond to reports with commitment. Low-threshold reporting systems are useful, but alone do not do justice to the extent of the problems. The number of unreported violations of consumer protection and criminal law that are never reported would be enormous, even with optimised reporting systems. Consumers rarely document negative experiences and even then do not always pass them on to platforms or consumer associations. Not to forget: dubious offers are not only found on specialized platforms but also on websites that can be found via search engines. Since general search engines usually take the view that they bear little responsibility due to a lack of proximity to the content, they are even more difficult to motivate to cooperate in law enforcement. Many violations of consumer protection standards relevant to criminal law, but also violations of civil and administrative law are not punished at all. The overwhelming number and the fact that the providers cannot be identified with reasonable effort means that no effective market surveillance is exercised. The governance structures (in Austria administrative criminal proceedings, warning proceedings initiated by consumer associations) are designed for localizable providers who cooperate seriously with authorities and courts. The procedures are unsuitable for the inexhaustible market of criminal offers. But even criminal investigation authorities do not see it as their primary task to investigate mass Internet fraud in view of the high investigation effort with low chances of success. Cybercrime statistics show the extent to which the total annual damage increases due to the deliberate disregard of consumer protection standards in enrichment intentions and common forms of Internet crime (see e.g. the Austrian Cybercrime Report <https://www.bmi.gv.at/news.aspx?id=6D4D326A543767595673593D>). According to the report, "Internet fraud encompasses" a multitude of modi operandi, ranging from the feigned delivery of goods to the promise of profit. More and more targeted forms of fraud are being developed, which can be carried out undetected and "safely" for the perpetrator through anonymization processes and concealment of financial flows. Criminals are able to address a broad public and turn them into potential victims. Frequently, order fraud using fake web shops, the use of false identities and contact details when making online purchases or fraudulent promises of financial investments are also a part of digital means of payment, such as Bitcoin or Ethereum.

## 14 How easy was it for you to find information on where you could report the illegal content/activity?

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



## 15 How easy was it for you to report the illegal content/activity?

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



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

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



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

- Yes
- No

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

*3000 character(s) maximum*

Since the COVID 19 pandemic, it has become apparent that there are pandemic-specific offers, such as fake protective masks that do not meet the necessary safety standards. Otherwise, no significant changes can be identified.

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*

In our experience, consumers find illegal goods through a simple internet search or through social networks. They assume that the offers are checked and controlled by the suppliers. This leap of faith leads them to open a search result thoughtlessly and/or click on an advertisement without question and order the illegal goods. A remedy may be that advertising for certain suspicious product groups may only come from reputable traders.

If consumers report an illegal product, the processing should not be limited to this specific report, but should include further tasks: Platforms should investigate whether, in connection with the report, other products are as well conspicuous which come from the same supplier/registrar. If the platforms discover noticeable problems, they are to block further offers that have not yet been reported or entire traders, independent of the specific report.

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*

Efforts within the company are beyond our knowledge. In any case, the results are insufficient. For example, the most popular app shops still do not ensure that allegedly free online games for young people contain reliable information on in-app purchases integrated into games before they are downloaded. The EU Commission has already addressed the issue of unfair business practices in 2014 ([https://ec.europa.eu/commission/presscorner/detail/de/IP\\_14\\_187](https://ec.europa.eu/commission/presscorner/detail/de/IP_14_187)) - apparently without success, as ongoing complaints in our advice centres show.

There are particular enforcement deficits with regard to prohibited direct invitations to children and young people to buy, missing correct legal information, advertising labelling, missing fee information on websites promising free use, prepayment fraud via fake shops for almost all categories of goods, countless streaming services (blacklist on <https://www.watchlist-internet.at/listestreaming-plattformen/>) that infringe copyrights and contain expensive subscription traps, and much more.

Especially fake shops are often hardly recognizable at first glance. Some of them are copying real existing websites, they seem serious and therefore rarely leave the buyer in doubt about their authenticity. With well-copied product images, fake quality labels and a professional appearance they gain the trust of online buyers and entice them to buy. Another lure is the apparently particularly low price of the product they are looking for. After prepayment, inferior goods are shipped at an inflated price or - far more often - the product is not delivered at all. If such a case is reported to platforms or authorities, ten more are opened at the same time. Part of the business practice is that the shops are quickly deactivated and re-registered under a new domain.

Therefore, reporting systems for platforms can only be a first step. To protect consumers, new ways of enforcing the law should also be promoted. In Austria, for example, there is a cooperation between science and consumer protection (Austrian Institute for Technology and the initiative "Watchlist Internet Fraud") with the aim of training algorithms to reliably detect fake shops and fakes of e-Commerce quality marks by means of typical features. The hit rate in the test phase is promising (<https://www.watchlist-internet.at/>; [www.ait.ac.at](http://www.ait.ac.at)). The use of such tools for the preventive protection of consumers is not an overburden for a platform.

With an EU-wide warning app (similar to the Austrian one) consumers should be able to assess the seriousness of websites according to fraud characteristics, which will be continuously updated. A green-yellow-red traffic light shows whether a website you have visited is trustworthy, should be critically questioned again or should not be used as a probable fake shop under any circumstances.

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*

According to consumer feedback, their announcements only produce a standard response, which for example refers in general terms to Community directives or conditions of use. If consumers reply to this pre-prepared message, they will only be informed that something is being checked against the guidelines/terms of use. There is no feedback on the content.

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*



Recommendations and rankings, as found on video and music streaming services, search engines or language assistants, are highly opaque. The factors influencing selection and ranking would have to be explained to consumers. If personal data are included, these would have to be disclosed. The GDPR contains no transparency obligations for recommendation systems. According to Art 22 GDPR (automatic decision making and profiling), only the data, logic, consequences of such systems that entail legal or similarly detrimental consequences for consumers would have to be described. An amendment to the Digital Service Act would improve the information situation and media competence of consumers and reduce the risk of manipulation. In the case of large platforms, users should also be able to make choices.

Consumers also do not know why they are shown an individualised advertising message. Paid premium positions on comparison portals and search engines are often not marked as advertising. The advertising networks behind an advertising placement are hardly recognizable. There is no possibility to cancel individualised advertising. Thus, a product once viewed tracks consumers over many websites and weeks. Anyone who wants to speak out in favour of "don't track" and against individualised advertising has no justifiable way of expressing this attitude simply and effectively. However, it would be reasonable for advertising networks to offer simple opt-out options. After all, income can also be generated with contextual advertising. The central "Robinson list" for unsolicited e-mail advertising to be set up under the e-Commerce Directive should become a "stop-tracking" tool for individualised online advertising. Imposed advertising completely misses the target of paying advertisers.

Requirements for commercial providers of rankings, comparisons and rating systems are missing. Competition law is available as a remedy against manipulation and deception. It is difficult to prove infringements of unfair competition law due to the lack of insight into the ranking practice. According to the Modernisation Directive (No. 11a Annex I UCP Directive n.F), "purchased" ranking positions without advertising labelling are prohibited. According to Art. 7 (6) UCPD n.F., providers must disclose whether and, if so, how they check whether ratings come from "real buyers". These rules are not sufficient. For example, it is estimated that one third of the ratings on the net are fake (see study at <https://www.arbeiterkammer.at/bewertungsplattformen>). Evaluation systems should therefore have to take measures to ensure that fake ratings are actually used. Comparable providers would have to prove their independence: Commissions, for example, must not affect the comparison result. Bonds can be taken from the international standard ISO 20488:2018 (Online Consumer Reviews), which contains requirements for rating systems.

### **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*

No, because it is always possible for children to log in to platforms with false data without verification: An age verification does not take place de facto, because children can confirm that they have reached a certain age with the push of a button, without anyone verifying this information. This is made more difficult by the fact that offers are usually pre-set in a data protection unfriendly way and profiles are therefore public. This is precisely what enables unknown third parties to contact minors and start harmful behaviour. In doing so, they exploit the inexperience of children as well as the data protection-unfriendly default settings of the platforms.

Regardless of this, it is apparent that platforms do not delete or block children's content if parents report it to the operator. This is disadvantageous because children often no longer know with which access data they have created a profile and can therefore remain online in the future. This, however, allows criminals to use pictures for prohibited purposes.

A further problem is that in the case of prohibited behaviour, each individual must be reported to the operator and the operator decides on a case-by-case basis and completely untransparent whether there is a violation of - usually - its guidelines, but not the law. This is disillusioning for victims, because although they already have to deal with prohibited actions anyway, there is not enough support from the platforms.

## 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	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
To protect freedom of expression online, diverse voices should be heard	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Disinformation is spread by manipulating algorithmic processes on online platforms	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online platforms can be trusted that their internal practices sufficiently guarantee democratic integrity, pluralism, non-discrimination, tolerance, justice, solidarity and gender equality.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

### 3 Please explain.

*3000 character(s) maximum*

In practice, it has been shown that consumers often report obviously dividing content, e.g. content that is directed against religious affiliation or political views, origin or gender, to platforms and want these removed. However, reporting this leads to a standard response and no deletion of the entry. Only when a real contact person at the platform - who is known through informal contacts - is informed of this violation will the entry be deleted. Nonetheless, the automatic algorithm often does not decide this way. Furthermore, it can be seen that messages are picked up but remain unprocessed over their very long period of time. Then it is often stated that the content does not violate the guidelines. National laws often play no role in decisions about this. This is a massive shortage.

### 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*

There are pandemic-specific contents that claim to know the truth about the coronavirus and the safety precautions. They are popular and are currently the gateway for further content that generally spreads conspiracy theories and so on.

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

*3000 character(s) maximum*

Reports of such content should be taken seriously and the content removed.

## **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*

Consumers report that their online accounts are blocked by providers without them knowing why. They often receive only a hint that there has been a policy violation. Blocking an account can lead to loss of credit or other digital services. This is not replaced for the consumers, so they are harmed once again. There is no procedure in which they can make their case and prove their innocence. How the wrong decision is made remains completely unclear to consumers.

---

***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*

If there is informal contact with online platforms can be reported and removed through this advertising for illegal content. However, this is often only a short-term success, because the advertising comes back again and again, so the problem would have to be reported continuously. However, therefore is often a lack of capacity and resources.

The Chamber of Labour obtains information about which contents lead to problems from consumers who have been victims of these illegal offers.

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

*3000 character(s) maximum*

No specific costs.

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*

Consumers are constantly pointing to illegal content originating outside the EU. For example, prohibited financial services, goods that do not comply with security standards, offers of forged documents, weapons, drugs or obviously criminal acts (e.g. money laundering or order fraud). Experience shows that victims cannot be helped in the event of direct damage. For this reason, preventive efforts are made to inform consumers about these illegal offers with all their disadvantages so that they do not become victims in the first place. This is done, for example, in the form of warnings, press work, social media activities or lectures /workshops.

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

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

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

*1000 character(s) maximum*

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*

First of all, we inform ourselves about a provider through an internet research. With this we pursue the purpose to find out whether someone is already known as dubious. If necessary, we also use a supplementary UID query or check the company codes/register of companies to find out whether the information given may actually be correct. Further approaches are a reverse image search - do photos appear in a different context and could they have been copied for illegal purposes?

Another approach is a Whois search. If a service has been registered via an anonymization service or has been carried out with obvious fake data, this is also an indication for us that something is incorrect.

The next step is to take a closer look at an online offer or profile. For example, does it comply with legal requirements or not. Depending on the answer to this question, this allows conclusions to be drawn about the seriousness.

Last but not least, it is also consumer reports that help the Chamber of Labour to draw conclusions about the seriousness of a provider. If these are negative, this is a strong indication that something is not right.

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

- Yes
- No
- I don't know

12 Please specify for what specific purpose and if the information available to you sufficient, in your opinion?

*3000 character(s) maximum*

See answer to question 10: "Another approach is a WHOIS query. If a service was registered through an anonymization service or performed with obvious fake data, this is also an indication that something is wrong." Within the EU, the fact that the owner data of a domain is not publicly available makes things more difficult. This prevents conclusions about whether an offer is serious or not.

13 How valuable is this information for you?

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



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

*3000 character(s) maximum*

See answer to question 10: "Another approach is a WHOIS query. If a service was registered through an anonymization service or performed with obvious fake data, this is also an indication that something is wrong." Within the EU, the fact that the owner data of a domain is not publicly available makes things more difficult. This prevents conclusions about whether an offer is serious or not.

*The following questions are targeted at online intermediaries.*

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

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

- A notice-and-action system for users to report illegal activities
- A dedicated channel through which authorities report illegal activities
- Cooperation with trusted organisations who report illegal activities, following a fast-track assessment of the notification
- A system for the identification of professional users ('know your customer')
- A system for penalising users who are repeat offenders

- A system for informing consumers that they have purchased an illegal good, once you become aware of this
- Multi-lingual moderation teams
- Automated systems for detecting illegal activities. Please specify the detection system and the type of illegal content it is used for
- Other systems. Please specify in the text box below
- No system in place

2 Please explain.

*5000 character(s) maximum*

3 What issues have you encountered in operating these systems?

*5000 character(s) maximum*

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

- Yes
- No

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

*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*

*The following questions are open for all respondents.*

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

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

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

	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)	Yes, only by larger online platforms	Yes, only platforms at particular risk of exposure to illegal activities by their users	Such measures should not be required by law
Maintain an effective 'notice and action' system for reporting illegal goods or content	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Maintain a system for assessing the risk of exposure to illegal goods or content	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Have content moderation teams, appropriately trained and resourced	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Systematically respond to requests from law enforcement authorities	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cooperate with national authorities and law enforcement, in accordance with clear procedures	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cooperate with trusted organisations with proven expertise that can report illegal activities for fast analysis ('trusted flaggers')	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Detect illegal content, goods or services	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
In particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Request professional users to identify themselves clearly ('know your customer' policy)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide technical means allowing professional users to comply with their obligations (e.g. enable them to publish on the platform the pre-contractual information consumers need to receive in accordance with applicable consumer law)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Inform consumers when they become aware of product recalls or sales of illegal goods	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cooperate with other online platforms for exchanging best practices, sharing information or tools to tackle illegal activities	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Be transparent about their content policies, measures and their effects	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Maintain an effective 'counter-notice' system for users whose goods or content is removed to dispute erroneous decisions	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other. Please specify	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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

*5000 character(s) maximum*

Platforms should have to follow the same guidelines regardless of their size. Because the need to protect consumers against manipulation, misleading, financial or health damage etc. is the same regardless of the size of the platforms. Many smaller, local switching platforms are operated with great care. Little effort is spared to subject commercial third parties to a thorough examination before they are accepted. Large platforms have comparatively unlimited means of carrying out automated checks (prior verification of the identity of commercial providers and the admissibility of their offers). If no size-independent ex-ante control obligations on operators were introduced, Member State authorities would alternatively have to be entrusted with more systematic controls of Internet offerings, but their resources would quickly reach their limits.

A differentiation according to the nature of the platform should be mandatory: for social media and, in general, services using user-generated content, obligations must be measured strictly against the fundamental right to freedom of expression and information. Art 15 of the current e-Commerce Directive has proved its worth and must be maintained unchanged with regard to platforms that store content relevant to fundamental rights. Accordingly, no general, preventive monitoring obligations may be imposed on operators with regard to the content stored or transmitted by them.

In the case of commodity trading and other intermediary platforms for commercial offers, there is considerably less reason for caution with regard to respect for the fundamental right to freedom of information and freedom of opinion. It goes without saying that the fundamental right to freedom of acquisition should not be restricted in the case of legally compliant offers. Here, the preventive protection of consumers at least through random, manual checks and technical means of detecting and filtering illegal business practices is of great relevance. An addition of a larger scope of liability for trading platforms in Art 15 of the E-Commerce Directive would be absolutely timely. Providers and their goods or services would have to be examined by the platforms according to various criteria. In the case of easily recognisable illegalities or uncertainties which the provider does not clear up by submitting documents, the third-party provider must be denied access. Consumers in online marketplaces are exposed to various risks of damage - they range from financial to health impairments (e.g. advance payment fraud, sale of counterfeit drugs that are hazardous to health). If platforms do not fulfil their obligation to clearly identify third-party providers on their platforms and not to activate fraudulent offers that are easily recognisable in the course of a preliminary examination, they should be liable for occurred damages on the consumer side due to their lack of due diligence.

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

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

4 Please explain

*3000 character(s) maximum*

Notification requirements should be low-threshold for consumers. Otherwise they would hardly be used. Notifying persons should explain their complaint in more detail, but as persons unfamiliar with the law, they should not be required to state the exact infringement. In contrast to delete requests due to violations of personal rights, there is no objective reason to query the identity of the person reporting (presumably) illegal business practices, content or product offers. Consumers should be able to choose whether they want to forward completed reporting forms to the platform or to the competent authorities at the same time.

The platform providers should in any case provide for appropriate forwarding options. Moreover, platforms should be encouraged to remove offers not only if they contradict the terms of use agreed with the providers, but also if they generally disregard legal norms.

Consumer organisations, which frequently submit reports with substantiated facts and a well-founded legal justification, should quickly be given the status of "trusted flaggers", which should trigger a predefined process (such as comments and remedial action by the platform within certain deadlines).

## 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*

The list of fraudulent streaming platforms (<https://www.watchlist-internet.at/liste-streaming-plattformen/>) illustrates that new websites with similar scams go online practically every day. Delete routines of platforms will always lag behind criminal practices. Nevertheless, platforms should be obliged to use algorithms not only for increasingly sophisticated consumer behaviour profiles, but also to control third-party providers on platforms and in search engine results. Above all, this includes to detect the repeated appearance of incriminated offers and commercial practices and to remove them again and again.

Furthermore, at least all major platforms should finance the establishment and ongoing operation of an EU-wide, independent warning platform for cybercrime. If illegal offers cannot be quickly sorted out before consumers see them, despite all efforts, then much more must be invested in consumer information. The Austrian initiative "Watchlist-Internet" can serve as a model (which is also co-financed by the BAK, see <https://www.watchlist-internet.at/>). Given the cross-border dimension of most forms of Internet fraud, a comparable EU-wide initiative is overdue. Its function would be to provide up-to-date information on a daily basis about forms of fraud reported on the Internet (by consumers, consumer organisations, platforms and authorities) and to give tips on how to protect oneself against common scams. By entering the internet address or the company name, consumers should be able to check whether an entry in the blacklist already exists in order to be protected from cost or data traps. Victims of Internet fraud should receive instructions for further steps. The platforms should not only support the project financially. They should also pass on their own perceptions of illegal practices on their platform for publication on the "watch list" and help victims who report to the watch list. In addition, given their technical expertise, they could promote the EU-wide development and distribution of consumer protection tools (such as a notification app on new watchlist entries or apps that detect fakeshops or quality mark counterfeits).

## 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 project of an automated fake-shop detection in Austria, which was accompanied by scientific research as described above, shows that machine learning systems are able to display new candidates for suspensions relatively accurately by continuously feeding in new fraud variants. Of course, platforms will not be able to prevent the re-emergence of blocked content 100%. However, an obligation to at least make reasonable efforts, document them and disclose them to the authorities should be provided for in any case. As repeatedly emphasised, "notice and take down" strategies by means of reporting systems are a useful, but not the most efficient method of keeping platforms as free as possible from illegal practices. Expedient would be to keep platforms in line with the "know your customer" principle, to check providers and their offerings in advance according to certain standards (identity declaration, representatives within the EU, random website screening and more precise checks for sensitive product categories). Provision should be made for the platforms to be liable for consumer damage if they have failed to comply with their defined prior checking obligations. This would ensure that consumers would be compensated for damages for the first time (as attempts to prosecute unknown offenders are impossible and also hopeless with criminal providers who can be investigated). It also motivates platform providers to pay more attention to who is allowed to offer goods and services on their platforms.

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*

The scope of application should cover all offers of goods, services and digital content that can be obtained by European consumers, whether for payment or free of charge, regardless of whether the company has a registered office within the EU. Art 3 in conjunction with EC 23 of the Basic Data Protection Regulation can serve as a model for this.

Furthermore, it must be ensured that suppliers from third countries which do not have an establishment in the EU must designate an authorised representative with an address within the EU who is capable of bringing an action. By analogy with Art 27 GDPR, the representative should be a natural or legal person established in the EU who has been appointed by the online provider in writing and represents the online provider with regard to the obligation to comply with EU law (consumer protection standards, trade law, etc.). The platforms should check whether authorised representatives exist at all at the address given and react if necessary. If platforms do not comply with this obligation, they themselves should be liable for damages to consumers resulting from the fact that they cannot hold any provider or authorised representative in the EU liable.

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*

Such far-reaching measures should only be considered if no remedy can be found at a higher level. First and foremost, it is the duty of the host provider to eliminate illegal content on its website. In the final analysis, domain blocks are conceivable in the case of continuous, serious violations or criminal host providers who refuse to cooperate.

## 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*

Platforms should be obliged not only to react to infringements by removing offers on their websites, but also to provide authorities (administrative, consumer protection, data protection and industry supervisory authorities) with documentation of the facts for further legal prosecution. NGOs that support consumers by advising them, arbitrate and settle disputes and conducting tests should quickly achieve a "trusted flagger" status. Following a defined process, they should quickly come into direct contact with a authorised decision-maker of the platform in order to negotiate rapid and satisfactory solutions for affected consumers.

Cooperation between Member State authorities of one or more countries should be significantly improved. Member States must demonstrate that they allocate sufficient resources to this end.

## 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*

The 35-year-old Product Liability Directive does not provide adequate answers with regard to distribution structures in online trade and contains unsatisfactory gaps in protection for consumers who purchase goods via platforms of traders or manufacturers based outside the EU (above all increasingly in China). Thus, joint and several liabilities should also be provided for the "fulfilment" service provider (storage, packaging, addressing and dispatch of products to which they have no ownership rights, with the exception of conventional postal services) in addition to the manufacturer (Art. 3 para. 1 Product Liability Directive) and the importer (Art. 3 para. 2 Product Liability Directive). However, joint and several liability, modelled on the importer's liability (Art. 3 para. 2 of the Directive on Product Liability), seems appropriate even for platform operators who do not provide fulfilment services. Insofar as platforms allow providers from third countries, the risk of a claim under the Product Liability Directive is reasonable. Otherwise consumers have absolutely no chance of enforcing legal claims for example against US or Chinese providers. With the help of algorithmic risk assessments, platform providers would certainly be able to prevent potentially dangerous products from being allowed on the online marketplace. They can also pass on such financial risks to their commercial platform users (for example, calculate the amount of commission according to whether the respective product poses a high risk) and take out risk insurance.

## 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*



Social media, app stores and online games providers offer children and young people far too little protection from online marketing. Despite the GDPR, e-privacy Directive and the Directive on Audiovisual Media Services, some large platforms continue to engage in illegal practices in data use and Advertising payout. Their efforts to encourage third party providers on their platform to behave in a legally compliant manner towards children and young people in this respect are correspondingly limited. For example, a study commissioned by the BAK showed that Facebook uses more than 30 different forms of advertising. In these cases, content is hidden and insufficiently marked as commercial communication, so that minors cannot be aware of the advertising content at all and are exposed to considerable risks of manipulation.

The restrictions on the usability of children's data in accordance with the GDPR are often disregarded by those platforms and third party providers that are particularly keen to be used by minors. And even video bloggers do not always find the tools they need on the most popular platforms for young people to correctly label their contributions as advertising (see e.g. the BAK study on influencer marketing, <https://www.arbeiterkammer.at/beratung/konsument/HandyundInternet/Internet/Videoblogger.html>).

Content that is not age-appropriate and contains violence, pornography, etc. is still accessible to children and young people. While conventional audiovisual media services are strictly regulated according to the EU Directive of the same name and are also largely controlled by supervisory authorities, this is by no means the case for offers on the Internet outside of large video-on-demand platforms such as YouTube.

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

	1 (not at all necessary)	2	3 (neutral)	4	5 (essential)	I don't know / No answer
Transparently inform consumers about political advertising and sponsored content, in particular during election periods	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with user complaints	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Tackle the use of fake-accounts, fake engagements, bots and inauthentic users behaviour aimed at amplifying false or misleading narratives	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Transparency tools and secure access to platform data for trusted researchers in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Transparency tools and secure access to platform data for authorities in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Adapted risk assessments and mitigation strategies undertaken by online platforms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Ensure effective access and visibility of a variety of authentic and professional journalistic sources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Auditing systems for platform actions and risk assessments	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Regulatory oversight and auditing competence over platforms' actions and risk assessments, including on sufficient resources and staff, and responsible examination of metrics and capacities related to fake accounts and their impact on the manipulation and amplification of disinformation.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other (please specify)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

### 13 Please specify

*3000 character(s) maximum*

Deliberate disinformation to manipulate public opinion and conduct targeted campaigns on highly emotionalising and divisive issues is undoubtedly essential in terms of democratic policy. Under no circumstances should it be ignored that consumers are also exposed to mass disinformation and manipulation. Behaviour-based marketing and psychologically strongly influencing forms of advertising are a determining part of the online business model. Behavioural profiles resulting from monitoring the Internet behaviour of consumers across all services and highly individualised advertising through microtargeting also have a manipulative effect and annoy the majority of consumers. A regulation of permissible online advertising forms and prohibition standards for non-transparent, manipulative marketing methods is overdue.

The concentration of data on a few large platforms and service providers in the online advertising market leads to abusive behaviour (e.g. complete lack of transparency towards consumers, serial data protection violations, unfair profit margins under competition law due to the monetization of data by the advertising service providers instead of the content providers).

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*

Online providers are to be obliged to report reported and self-observed violations to authorities. Consumers and consumer associations who report infringements to platforms should find a link on the platform where they can immediately forward the content of the completed report form to the competent authorities.

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

	1 (not at all necessary)	2	3 (neutral)	4	5 (essential)	I don't know / No answer
High standards of transparency on their terms of service and removal decisions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Diligence in assessing the content notified to them for removal or blocking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Maintaining an effective complaint and redress mechanism	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Diligence in informing users whose content/goods/services was removed or blocked or whose accounts are threatened to be suspended	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

High accuracy and diligent control mechanisms, including human oversight, when automated tools are deployed for detecting, removing or demoting content or suspending users' accounts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Enabling third party insight – e.g. by academics – of main content moderation systems	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other. Please specify	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 16 Please explain.

*3000 character(s) maximum*

In the case of social media and in general platforms based on user-generated content or similar or equivalent to traditional communication services, the prohibition of general monitoring obligations under Article 15 of the e-Commerce Directive should be maintained. Freedom of opinion and information as well as respect for the confidentiality of communications are particularly important in this case.

There should only be limited exceptions to this principle: With regard to commercial advertising (which is also played out on platforms sensitive to fundamental rights with user-generated content), a general obligation to carry out a general prior check without any fundamental rights concerns can and should apply: compliance with labelling obligations under advertising law, removal of obviously illegal content. With regard to communication platforms such as social networks, there is currently a particular concern that providers are reacting to public pressure and the prospect of very high punitive sanctions by not only deleting incriminated content more quickly (see e.g. German Network Enforcement Act) but also by deleting excessive behaviour, i.e. by "overblocking" too much in cases of doubt. It goes without saying that the platforms must be given instructions to block or delete illegal content immediately after they have been informed of it. But there is also a need for compensation mechanisms to ensure that legitimate contributions are not deleted from the net. It would therefore be useful to have national, independent arbitration bodies which would make decisions on a case-by-case basis, weighing up the conflicting interests of freedom of expression and data protection or personal rights. Access to review by the courts must be open to participants in conciliation proceedings. In addition, platforms must be obliged to transparently disclose algorithm-controlled decision-making processes regarding the remain or removal of content and to make documentation of their individual decisions available to competent authorities (data protection, media, criminal law authorities, etc.).

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*

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*

The personal data, criteria and, in general terms, the logic of filtering systems should be accessible for everyone. In addition, new supervisory authorities should be established or existing supervisory authorities should be given the additional task of algorithmic control with regard to the scientific verifiability and durability of results, respect for fundamental rights, non-discrimination, transparency requirements and an independent dispute settlement body. In the case of applications subject to prior authorisation or in the case of verifying controls, all details of the use of algorithms must be disclosed to these bodies.

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

*5000 character(s) maximum*

Recommendations and rankings, such as those found on video, film and music streaming services, search engines or language assistants, are characterized by a lack of transparency. The factors influencing the selection and ranking would have to be explained to consumers. If personal data are among the influence factors, they should be disclosed. The GDPR contains no transparency obligations for recommendation systems. According to Art 22 GDPR (automatic decision making and profiling), only the data, logic, consequences of such systems that entail legal consequences for consumers or similar adverse effects are to be described. An amendment to the Digital Service Act would improve the level of information and media competence of consumers and reduce the risk of manipulation. Users should also be able to make choices (deactivation of recommendations, ranking according to criteria of personal preference). Consumers also do not know why they are shown an individualised advertising message. Paid premium positions on comparison portals and search engines are often not marked as advertising. The advertising networks behind an advertising placement are hardly recognizable. There is no possibility to cancel individualised advertising if consumers find it annoying. A product once viewed, for example, follows consumers over many websites and weeks. Those who wish to make a general "don't track" statement of intent and do not appreciate individualised online advertising have no reasonable way of expressing this attitude simply and effectively. It is reasonable for advertising networks to offer simple opt-out options. After all, income can also be generated with contextual advertising. The central "Robinson list" for unwanted e-mail advertising to be set up under the e-Commerce Directive should become a genuine "stop-tracking" tool for every form of online advertising. Imposed advertising completely misses the target of paying advertisers anyway.

Requirements for commercial providers of rankings, comparisons and rating systems are missing. As a remedy against manipulation and misleading, competition law is at disposal. It is difficult to prove infringements of unfair competition law due to the lack of insight into the ranking practice. According to the Modernisation Directive (No. 11a Annex I UCP Directive n.F), "purchased" ranking positions without advertising labelling are prohibited. According to Art. 7 (6) UCPD n.F., providers must disclose whether and, if so, how they check whether ratings come from "real buyers". These rules alone are not sufficient. Rating systems should actually have to take measures against fake ratings bought by agencies. Comparable providers would have to prove their independence: For example, commissions should not affect the results of the comparison. Bonds can be taken from the international standard ISO 20488:2018 (Online Consumer Reviews), which contains requirements for rating systems.

The personalisation of offers by individualisation of the price must be made clearly visible to consumers (see obligation of the Omnibus Directive). However, consumers must also be given a more detailed description of the consequences. Otherwise they will not be able to form an adequate picture of possible disadvantages: Person A will be shown cheaper offers compared to person B, the preset sequence of offers is different for person A than for person B, etc. Certain forms of algorithm-controlled individualisation of offers should be prohibited in general: for example, the target group size should not be allowed to fall below a certain number of persons. Offers should not be broken down to a single determinable person. The criteria for a different treatment of certain target groups must not be unobjective, discriminating. The use of such personalisation systems and the website information about them intended for consumers should be subject to prior checking by supervisory authorities responsible for algorithmic controls and data protection. Additional requirements regarding consumer protection when using algorithms can be found in our opinion on the White Paper on Artificial Intelligence: <https://www.arbeiterkammer.at/kuenstlicheintelligenz>.

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*

There is currently no comprehensive regulatory review of how platforms deal with national legal requirements. The information they provide (e.g. in transparency reports) is rarely informative and is not subject to closer regulatory scrutiny. The GDPR should not be an obstacle to national authorities requesting the data they need to fulfil e.g. their tax and municipal obligations. If necessary, a corresponding permit should be created.

## 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*

In addition to administrative penalties for failure to comply with exercise rules, transparency and inspection obligations, new liability regulations are also under consideration. In the case of intermediary platforms - such as online marketplaces - consumers are exposed to a variety of considerable risks of damage - ranging from financial to health impairments (from advance payment fraud to online sales of counterfeit, health-endangering drugs). If platforms do not comply with their obligation to clearly identify third-party providers on their platforms and not to activate fraudulent offers that are easily identifiable in the course of a preliminary examination, they are due to their lack of due diligence themselves liable for the damage, guarantees, warranty defects etc. occurred by consumers.

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

*3000 character(s) maximum*

A summary of our consumer concerns regarding the future Digital Service Act is available at: [https://www.akeuropa.eu/sites/default/files/2020-05/DE\\_%C3%9Cberarbeitung%20der%20Richtlinie%20zum%20elektronischen%20Gesch%C3%A4ftsverkehr.pdf](https://www.akeuropa.eu/sites/default/files/2020-05/DE_%C3%9Cberarbeitung%20der%20Richtlinie%20zum%20elektronischen%20Gesch%C3%A4ftsverkehr.pdf)

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

---

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

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

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

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

5000 character(s) maximum

For hosting services, the disclaimer of liability for third party content or activities is based on the state of knowledge of (i.e. if the service providers have "actual knowledge" of the illegal activities, the service provider received, they must "take immediate action" to remove them, otherwise they could be held liable). This limitation of liability has been applied to social media and other platforms, based on user-generated content, with a view to protecting freedom of expression and information and the protection of privacy.

Intermediary platforms and search engines, which provide commercial offers from third parties (be it goods, services or digital content), advertising, ratings and comparisons on their sites, should be subject to stricter liability rules. Fundamental reservations against preventive, prior checking obligations do not apply here in this form. The need for a modern liability regime for consumer protection is obviously necessary. The platforms monitor activities in any case in terms of consumer behaviour and also curate the contents via recommendations and sequencing of offers. In view of this permanent control, it is not just about transmitting or storing content. We do not believe that liability privileges in the event that providers prove that they have taken voluntary, proactive measures is appropriate. An excellent liability regime that protects the interests and the possibilities of both parties to the agreement, has already been taken into account by a science team is working on it: [https://www.europeanlawinstitute.eu/fileadmin/user\\_upload/p\\_eli/Publications/ELI\\_Model\\_Rules\\_on\\_Online\\_Platforms.pdf](https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf)

Platform operators must themselves take responsibility for compliance with EU rules (by joint and several liability of the platform for violations of the rights of the third party providers or on the advertising spaces made available). Thereafter the jointly and severally liable joint liability of the platform provider if the consumer "can reasonably expect that the platform operator has a dominant influence on the supplier". This precondition is elaborated by a list of criteria.

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

We would like to refer to the non-exhaustive list of the European Law Institute (see also Point 2 above) with examples of online marketplaces that should be more strictly accountable because

- the consumer contract is concluded exclusively on the platform;
- platform provider restrain certain identity details about the third-party provider until the completion of the consumer contract
- the platform provider offers systems for the processing of payments
- the platform provider's general terms and conditions of business, which regulate the conclusion of contracts between third party providers and consumers, dictates or influences the price fixing
- the platform provider defines the rules of conduct of the third party providers in its general terms and conditions and monitors them, and much more.

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



The E-Commerce Directive already contains a so-called "notice and takedown" procedure. Internet provider can benefit from a liability exemption if they remove or block the access to information as quickly as possible as soon as they become aware of their unlawful character. The rules apply to any kind of illegal or unlawful content. However, service providers should not act as Internet police and providers who use user-generated content may not be forced into a general, active monitoring of this content. "notice and action"-mechanisms have a direct impact on freedom of opinion. Currently the access and host operators must decide when and how content is removed from the network They often have to decide on competing rights and interests. Since companies can't replace courts in this task, a "privatised law enforcement" should be in case of user-generated content, such as social media, blogs or forums be rejected. In the event of a dispute over an independent arbitration of disputes - in addition to the courts - should be established to deal with any blockage, whether or not it has been enforced can be called. In the case of platforms that offer commercial offers from third parties (goods, services, digital content) would also be subject to mandatory prior checks on the legality of the providers and their offers for the preventive protection of consumers are appropriate. See with regard to this "Good Samaritan" approach, which is misguided from the consumer's point of view, for example the Study by the European Parliamentary Research Service ([https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS\\_IDA\(2020\)649404\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_EN.pdf)).

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*

At least the platforms relevant for consumers all play an active role.

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 maxim that Internet access and host providers should not be subject to general, blanket ex ante obligations in the case of to impose situations affecting fundamental rights should be maintained (Art 15 e-Commerce RL). When weighing up the pros and cons of preventive filtering measures, the concerns regarding associated restrictions on fundamental rights and freedoms under the ECHR by far. The Scope for "proactive measures" (essentially an algorithm control) such as the regulation on the fight against terrorist content online, should under no circumstances be replaced by other specific derogations of Art 15 should be extended.

However, as has been pointed out several times, many situations do not affect fundamental rights to freedom of expression and information, data protection and privacy. A preventive one, a general duty to monitor companies, their offers and advertising in relation to their legal conformity is probably one of the due

diligence obligations of intermediary platforms, which they must fulfil in cooperation with the competent authorities, the criminal law, trade and tax law, municipal legal regulations, labour law, consumer and data protection law, etc.

## 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*

As repeatedly emphasised, the liability relief provided by the e-commerce rules has proved its worth in many sensitive areas of application in terms of fundamental rights. This is not opposed to an addition in reference to a stricter liability of online marketplaces that mediate commercial offers or provide advertising services. Against this background, the future rules for host providers distinguish which content is "hosted".

Yes, the 35-year-old product liability directive does not offer any protection with regard to the distribution structures in online trade. Adequate responses and contains unsatisfactory gaps in protection for consumers who purchase goods via platforms of dealers or manufacturers based outside the EU (particularly increasingly in China) acquire. Thus, joint and several liability should also apply to the "fulfillment" service provider (storage, packaging, addressing and dispatch of products to which they have no right of ownership except for traditional postal services) in addition to the manufacturer (Art. 3 para. 1 of the Directive on Product Liability) and the importer (Art. 3 para. 2 Product Liability Directive). But even towards platform operators who do not provide fulfillment services, a joint and several liability appears in line with the model of the importer's liability (Art. 3(2) of the Directive on product liability). As far as platform providers from third countries, they are exposed to the risk of being taken up under the product liability directive. Otherwise consumers have absolutely no chance, to enforce legal claims against e.g. US or Chinese suppliers. Platform providers would be able to use algorithmic risk assessments (e.g. drugs, electrical appliances from certain third countries, etc) are quite capable of preventing dangerous products from entering the marketplace in the first place to be allowed. They may also transfer such financial risks to their commercial platform users (e.g., calculate the amount of the commission according to whether the product in question carries a high risk) and take out risk insurance. For the same reason, it would also be necessary to encourage platform providers to offer products that security requirements of the EU, not to unlock on their platform. Suppliers and products which, according to a general risk assessment, pose a high risk (country of origin without legal security standards corresponding to EU requirements, risk-prone product groups), must undergo a preliminary check before they can be placed on the platform can be unlocked.

## 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.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
It is easy for consumers to switch between services provided by online platform companies and use same or similar services provider by other online platform companies (“multi-home”).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
It is easy for individuals to port their data in a useful manner to alternative service providers outside of an online platform.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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

often poses a risk of reducing innovation and deterring competition from smaller innovative market operators.



**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*

Tax optimisation and precarious employment contribute to the high financial strength of digital companies. Both from the consumer's and the company's point of view the low or difficult (partly only hidden on the homepage) accessibility for inquiries and complaints has to be pointed out.

## 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*

The mentioned criteria can be combined in many ways by the large platforms due to their strong market position and financial power (e.g. also through acquisitions) and thus strengthening the gatekeeper function.

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

- online intermediation services (i.e. consumer-facing online platforms such as e-commerce marketplaces, social media, mobile app stores, etc., as per [Regulation \(EU\) 2019/1150](#) - see glossary)
- search engines
- operating systems for smart devices
- consumer reviews on large online platforms
- network and/or data infrastructure/cloud services
- digital identity services
- payment services (or other financial services)
- physical logistics such as product fulfilment services
- data management platforms
- online advertising intermediation services
- other. Please specify in the text box below.

## 5 Other - please list

*1000 character(s) maximum*

## Emerging issues

---

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

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

- Yes
- No

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

*5000 character(s) maximum*

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

*5000 character(s) maximum*

---

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

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

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

*5000 character(s) maximum*

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

*3000 character(s) maximum*

*The following questions are open to all respondents.*

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

*5000 character(s) maximum*

The problem if the platform offers a service for third parties and at the same time uses the platform for own offers in the function as a competitor. Intransparency (e.g. with algorithms).

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*

The use of third party customer data for own business activities.

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

*3000 character(s) maximum*

Competitors are forced out of the market and competition is influenced in their own favour. For consumers, this means less choice, less innovation and, in the long term, higher prices.

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*

Network effects and a critical mass of users are required. Also problematic are "killing mergers", in which innovative start-ups are bought up early and taken out of the market.

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 basically contribute to media diversity, but they do not offer the editorial independence with corresponding duties of care and control (e.g. with regard to fake news). Through algorithms based intransparent information selection, the diversity of opinions can be severely limited.



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*

Platforms must comply with a stricter editorial duty of care for media-specific content. This would also strengthen the quality of media and opinion diversity.

## **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*

Numerous competition proceedings, especially against the major online platforms, both on EU and national level, indicate the existence of market failures in this area. Competition law alone is always a (big) step behind and the procedures take a lot of time as well. From an economic point of view, only an ex-ante regulation can help to protect against negative economic impacts. Also with regard to negative social effects (e.g. freedom of expression, false and hate reports) there is more efficiency necessary.

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*

Prohibition of algorithms that have a discriminatory effect. Restrictions with regard to excessive data use and data linkage should be considered when the balance there is a gap between the giving of data and the possibilities of use.

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*

The following regulatory tasks could be envisaged: Non-discriminatory access to platforms ensure, regulation of the costs of access, regulation of data interfaces, control general terms and conditions, dispute settlement mechanisms (ombudsmen), production of data transparency and transparency of algorithms, Code of Conduct with regard to the use of personal data, obligatory reference in the application of personalized offers (in the prices, cooperation with data protection authorities, restrictions on excessive data use and data linkage, market structure analyses; sanction options).

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*

An independent and independent sectoral authority would be able to develop specific know-how and a sound knowledge of the markets the necessary implement regulatory measures rapidly.

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*

prohibition orders, fines and periodic penalty payments - analogous to competition law, structural regulations and behavioural requirements.

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*

See answer 8.

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*

Preference should be given to a single regulatory authority. However, the agendas of a already existing regulatory authority should be expanded and used. A mutual information exchange with other authorities (e. g. data protection, consumer protection, competition) is to be provided. Mutual consideration must be established for decisions, so that there are no conflicting decisions.

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*

It is necessary to establish appropriate cooperation mechanisms and to ensure that decisions are taken on the basis of a to establish mutual consideration. In principle, this can be done in a network to be founded can be made. Cooperation with the competition authorities, the consumer protection organisations and data protection authorities is urgently needed.

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*

Both effects should be addressed.

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*

With regard to personal data in particular, the GDPR must be further developed, including an effective means of law enforcement must be respected. With regard to platforms, it should strict regulations with regard to "privacy by design" and "privacy by default" and always the principle of data economy applies. A voluntary commitment by companies is to be little and has so far not proved successful. Furthermore, the distinction between personal and to sharpen non-personal data. Many (in themselves non-personal or anonymised) data can be analysed and merged to create a personal reference to the person concerned received. It is therefore necessary to define from when data can actually be considered non-personal apply. Users must also always have the possibility of processing their data agree or disagree with them. This also requires the greatest possible transparency, which is also the case with the use of algorithms must apply. All algorithm-based decisions, services and products must remain explainable and verifiable. Data and privacy protection should protect economic interests proceed in principle.

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*

As far as (algorithm-based) pre-selection is necessary to enable users of the platforms to should not be done for commercial reasons and, above all, should always be transparent. The means that users must also always have the choice to determine what is best for them is shown. Even though it should not be misunderstood that platforms are also have responsibility to combat fraud, the spread of fake news, hate and hate speech. Here there is a need for a clear mandate and legal framework for platform operators such as to deal with the spread of fake news and hatred and also individual opportunities for users quickly against insulting, discrediting, discriminating or untrue allegations their person.

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

- Institutional cooperation with other authorities addressing related sectors – e. g. competition authorities, data protection authorities, financial services authorities, consumer protection authorities, cyber security, etc.

- Pan-EU scope
- Swift and effective cross-border cooperation and assistance across Member States
- Capacity building within Member States
- High level of technical capabilities including data processing, auditing capacities
- Cooperation with extra-EU jurisdictions
- Other

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

*3000 character(s) maximum*

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

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

23 Other – please list

*3000 character(s) maximum*

Appropriate sanction mechanisms - analogous to competition and other regulatory law; improved possibilities for law enforcement, especially with regard to data protection rights.

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

*3000 character(s) maximum*

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

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

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

*3000 character(s) maximum*

A combination of the options 2 to 4 presented are complementary and should be considered as appropriate measures be newly established.

27 Are there other points you would like to raise?

*3000 character(s) maximum*

It is welcomed that the EU Commission is taking up these important issues and has launched a new competitive framework for current and future challenges. The new competition instruments under discussion (ex-ante regulation, new competition tool, and reform considerations on market definition) can help to ensure that currently existing competition deficits can be solved quickly and efficiently and that future developments can be examined more closely. This would allow early intervention to ensure fair competition.

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

---

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

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

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

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

### Online advertising

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

- Yes, always
- Sometimes: but I can find the information when this is not immediately clear
- Sometimes: but I cannot always find this information
- I don't know
-

No



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

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

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

*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 through real-time bidding		
Private marketplace auctions		
Programmatic advertising with guaranteed impressions (non-auction based)		
Behavioural advertising (micro-targeting)		
Contextual advertising		
Other		

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

*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*

We consider measures in the opposite case to be much more urgent: consumers surf on serious websites and receive dubious advertising (for fake shops, counterfeit goods, subscription or financial investment rip-offs, fraudulent lotteries, prohibited content and much more). About the intrusion of such advertising, they are led to short-term active, eg fraudulent websites.

Substantiated messages to platforms and website owners are excluded in this case. In view of the currently completely non-transparent advertising play-outs (who, when, on which order, on basis of which user data, how accessible, how can be cancelled in favour of contextual advertising) advertisements from consumer organisations or public authorities which are displayed briefly for consumers neither document verifiably nor identify the advertising networks responsible for it.

Websites and platforms that offer advertising space usually have no idea with which illegal advertising content can be played on their surfaces. Mere reporting systems can be used in relation to illegal advertising therefore rarely contributes to law enforcement. For example, the Austrian Advertising Council complaints in this regard, may be refused in the case of undocumented, cross-border or no responsible for attributable advertising is naturally not helpful.

Prevention would therefore also be a priority here. The factors involved in the automated auctioning of advertising space participants are currently subject neither to explicit testing and filtering obligations nor to strict market supervision. It would be important to ensure that advertising for at least obviously illegal content consumers are not reached at all. Hotlines for incriminated advertising could be based on complaints at least provide feedback that due to new illegal practices and content automated filters are to be sharpened.

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

*3000 character(s) maximum*

Consumers should be able to see clearly in all advertising what criteria led them to get this advertisement displayed. Consumers in general and for each insertion must have the possibility to unsubscribe from an individualised "microtargeting" advertisement or to choose from other, more criteria, including only contextual advertising placements.

In addition, the client of the advertising and the advertising network playing the game are of course clearly visible and in each case with contact details. Consumers can turn to these two, if they have complaints about the content of the advertisement or the advertising practice (e.g. encouraging children to buy on a website typically aimed at children, etc.)

According to the Omnibus Directive, paid positions in rankings or search engine rankings are also to be marked as advertising. Here too it must be disclosed which service was compensated and who is the client.

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

*3000 character(s) maximum*

A BAK test shows that not all audiovisual video retrieval platforms offer Influencer tools to mark the promotion of products as advertising ([https://www.arbeiterkammer.at/beratung/konsument/HandyundInternet/Internet/Influencermarketing\\_2018.pdf](https://www.arbeiterkammer.at/beratung/konsument/HandyundInternet/Internet/Influencermarketing_2018.pdf)). Platforms that provide such tools apparently do not check if they are used. Thus, neither the platforms nor the supervisory authorities of most Member States check systematically whether, for example, such videos are identified as advertising. Enormous enforcement deficits and manipulative incentives to buy for the main target group – young people – are the result.

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

*3000 character(s) maximum*

The online advertising industry itself frequently violates EU law. See for example the BEUC's published study of the Norwegian Forbrukerradet: <https://www.beuc.eu/publications/eu-consumer-groups-urgeimmediate-investigation-systematic-breaches-gdpr-online>. The study complains that the investigated advertising networks systematically violate the basic data protection regulation (GDPR). Against the background, we see it as one of the central tasks of legal policy to critically examine business models for access to online content. Infringements of data protection are indeed not an immediate subject of the future Digital Services Act. Very well to be addressed are intransparency and the business models based on data. They allow consumers, contrary to what is stated in the GDPR, no other choice but to accept escalating data use to get access to content. These systematic data protection violations are unacceptable to the EU and its commitment to the rule of law.

At least a general central opt-out system must ensure that consumers not against their will are exposed to advertising methods based on surveillance tracking, education unlimited behavioral profiles and prognoses and individualised "microtargeting". A consent or withdrawal on each individual website and service is required for consumers in any way reasonable. As a consequence of refusing consent, the access to services is often restricted or denied for consumers. Such business models are thus based on the GDPR ineffective - because not voluntarily given - declarations of consent by consumers. The naturally justified interest in a remuneration of the content offer can also be achieved by the insertion of contextual advertising or payment offers.

Since advertising for dubious or fraudulent services is becoming more prevalent, the responsibility in chain advertising service providers and platforms must be clarified. Since platforms are based on behavioral profiles of its users and a participation in the advertising revenues in the marketing practices of online advertising are involved, they should be heavily involved in illegal advertising. You should provide tools for the clear identification of advertising and its sponsors, which should be must be used by advertisers. In addition, they should avoid advertising on obvious (fake shops, prohibited goods, especially pirated goods, data theft, distribution of malware etc) must be automatically checked in advance. In contrast to other content in the case of advertising content, there is hardly any risk that automated filters could lead to the loss of information and data protected by basic rights personal rights are violated. Other websites with third-party advertising must at least establish a complaints mechanism.

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*

The above-mentioned advertising principles (labelling, separation, disclosure of the principal) will systematically be broken, because efficient control and tangible sanctions are almost completely lacking. Consumers are not only exposed to intransparency, manipulation, harassment and illegal advertising content. Traditional print and audiovisual media, which by and large follow advertising rules are grossly disadvantaged by unfair online advertising forms or content. Strict supervision and sanctions against violations must therefore be an important cornerstone of the Digital Services Act. The provision of both roles of platforms as "gatekeepers" and simultaneously data collecting advertising networks represents an unparalleled concentration of power. If the standard business model is set to context-based advertising, consumers benefit from the fact that finally their "don't track" will and data protection is respected. But new, innovative competitors also benefit, because the inappropriate alliance of platform provider and microtargeting driving advertising network is dissolved.

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

*3000 character(s) maximum*

To really do justice to the right of self-determination of internet users, the Robinson-list for e-mail advertising has to become a true "stop tracking" tool for behavior-based, individualised online advertising. A centrally managed opt-out option is currently only available for unsolicited set up mail advertising. Those who do not appreciate online advertising as a whole, but feel it is a nuisance, currently has no reasonable means of expressing this position simply and effectively. Intermediaries from the online advertising industry earn money from forced advertising. However, it fails to fulfil the objectives of the client with internet users who are not advertising-savvy completely. At present consumers have to struggle at every service in an unacceptable way with endless explanations, difficult attitudes and enormous deficits in data protection implementation. Who does not want that its digital traces are tracked for advertising purposes across the Internet, should have the possibility to register into a central list. All advertising networks must respect this opt-out request. Usually the content providers can achieve reasonable revenues with contextual advertising. With high-quality content, a pay-wall can of course also be set up. However, it would be inadmissible in this case alternatively, to provide for "figures with unlimited data". Consumers must be informed about the exact data scope so that they can choose between variants confidently and informedly. Between the monetary value of the data volume and the monetary amount for the access service there must also not be a striking disproportion. Moreover, it is high time for a uniform, strict level of regulation of online advertising regardless of which pages the advertisement is played on. So far there are only a few detailed rules for advertising in audiovisual media. For consumers it is completely irrelevant on which website or app they are staying. They always have the same need to protect themselves from intransparent, aggressive, to protect health, the environment or advertising harmful to young people, etc.

**Smart contracts**

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

--	--

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



## 2 Please explain the difficulties you perceive.

*3000 character(s) maximum*

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

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

## 4 Please explain.

*3000 character(s) maximum*

## 5 Are there other points you would like to raise?

*3000 character(s) maximum*

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

---

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



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

## **Relationship with the platform and the final customer**

1 What type of service do you offer through platforms?

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

2 Please explain.

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

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

- Yes
- No

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

- Yes
- No

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

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

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

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

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

*3000 character(s) maximum*

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

*3000 character(s) maximum*

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

*3000 character(s) maximum*

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

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

- Yes
- No

15 Please explain.

---

*The following questions are targeting online platforms.*

### **Role of platforms**

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

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

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

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

- Yes
- No

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

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

### **Rights and obligations**

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

*3000 character(s) maximum*

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

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

25 Please explain.

*3000 character(s) maximum*

---

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

*3000 character(s) maximum*

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

*3000 character(s) maximum*

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

- Yes
- No

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

*3000 character(s) maximum*

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

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

*3000 character(s) maximum*

---

*The following questions are open to all respondents*

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

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

	1 (no improvements needed)	2	3	4	5 (substantial improvements needed)	I don't know / No answer
Earnings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Flexibility of choosing when and /or where to provide services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Transparency on remuneration	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Measures to tackle non-payment of remuneration	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Transparency in online ratings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Ensuring that individuals providing services through platforms can contact each other and organise themselves for collective purposes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Tackling the issue of work carried out by individuals lacking legal permits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Prevention of discrimination of individuals providing services through platforms, for instance based on gender, racial or ethnic origin	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Allocation of liability in case of damage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Other, please specify	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

### 33 Please explain the issues that you encounter or perceive.

*3000 character(s) maximum*

The Federal Chamber of Labour (BAK) had to observe in meetings with affected persons and in the ongoing information sharing with the trade union organisations that the working conditions on digital platforms has very often to be described as precarious. This applies for example for questions of minimum wage, working time and workplace (for example, in some cases the working materials have to be provided by the workers). This situation exists or has existed, inter alia, for food delivery staff and transport agencies and is active in downstream areas such as parcel services. Only on February 18, 2020, there was a raid in Austria, in which 36 subcontractors were controlled by Amazon. In 49 cases, violations of labour law have been determined. Cases of bogus self-employment are often found with online platforms, i.e. there were criteria which prove that the person is in paid employment. On a positive note, it should be noted that in Austria, a sectoral collective agreement was concluded with a food delivery company. Also a works council could be elected there. In the case of a driving agency, national regulations a level playing field with taxis should be established. The solution to these two cases could well be a role model for other areas of online platforms.

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*

Employees in the online industry lack a legislative framework and usually a collective or collective agreement which could give them legal certainty. This is a major difference to traditional economy. The gaps in the legal system also lead to competitive disadvantages for traditional economy.

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*

Necessary minimum standards for platform workers:

- A provision is required which is based on the (rebuttable) presumption that an employment relationship exists with the platform as an employee. The reason for this requirement is that it is very difficult to obtain a transparent insight into the work organisation of the platforms. However, this is decisive for the assessment of whether an employment relationship is present. Another possibility would be the creation of a catalogue of indicators containing criteria that determine whether an employment relationship with a platform exists.
- Clarification that in the case of an employment relationship, employee protection provisions and collective agreements, collective bargaining agreements or minimum wage regulations apply.
- Clear regulations that in the case of an employment relationship the platform is responsible for the payment of the payroll tax, social security contributions and all other wage-related charges.
- Information obligations of platforms towards authorities and social security institutions also if there is no employment relationship with them but with the beneficiaries.



Other points which would improve the situation of employees and self-employed persons:

- The establishment of information obligations of the platform towards persons who are working for the platform.
- The remuneration of self-employed persons may not be lower than the minimum wage or the collectively agreed minimum wage for the same or similar activities as an employed person.
- Application of the right to equal treatment and the obligation of equal pay
- Standby times and search times must also count as working time.
- The use of competition and exclusivity clauses must be prohibited.
- Clauses that allow unfounded exclusion when contracts are awarded and unfounded rejection of work results must be prohibited.
- Disclosure of how ratings of platform workers emerge, including the possibility to correct falsified ratings.
- To create a free arbitration procedure for the settlement of disputes.

On the situation of employees in the offline or traditional service sector: gaps in

Legislation on online platform employees must be closed quickly. This is the only way a level playing field and an improvement in the situation of employees in the offline and online working places can be reached.

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*

Collective bargaining must be comprehensive and cover all areas. If collective bargaining and if collective agreements are only agreed in individual areas, there is a risk that the platforms will switch to other areas where no such agreements exist.

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

*3000 character(s) maximum*

There is a strong case for collective bargaining and collective agreements: They bring workers planning security and are an important element for companies for fair competition, where individual groups of companies no longer enjoy advantages at the expense of employees and all other companies.

40 Are there other points you would like to raise?

*3000 character(s) maximum*

The large digital platforms in particular are exploiting the existing gaps in EU legislation to gain advantages at the expense of employees and most other companies, which lead to a significant distortion of competition. In the coming years, the digital industry is expected to continue to grow and the creation of appropriate legislative regulations is therefore essential, especially for employees of online companies. The legal framework at EU level must include the following points with regard to platform workers:

- The statement that in case of doubt an employment relationship as an employee with the online platform exists.
- Collective bargaining agreements or minimum wage regulations apply.
- The same employee protection provisions apply as in traditional business sectors.
- The platform is responsible for the payment of wage tax, social security contributions and all other wage-related charges for its employees.
- Information obligations of platforms towards authorities and social security institutions – also if there is no employment relationship with them but with the beneficiaries.
- To avoid wage dumping, it must be ensured that the remuneration or fees for self-employed persons, may not lie down among those employed persons who perform the same or similar activities.
- Application of the right to equal treatment and the obligation of equal pay.
- Standby times and search times must also count as working time.

- The application of competition and exclusivity clauses and all other unfair clauses in employment contracts or contracts with self-employed persons must be excluded from the outset.
- Disclosure of how ratings are made on platform workers, including the possibility to correct falsified ratings.



## 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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Requirements to have a legal representative or an establishment in more than one Member State	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Different procedures and points of contact for obligations to cooperate with authorities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other types of legal requirements. Please specify below	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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

- Yes
- No
- I don't know

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

- Yes
- No
- I don't know

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

*3000 character(s) maximum*

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

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

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

- Yes
- No
- I don't know

14 Please explain

*3000 character(s) maximum*

*The following questions are targeted at all respondents.*

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

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

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

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

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

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

*5000 character(s) maximum*

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

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

	1 (not at all important)	2	3 (neutral)	4	5 (very important)	I don't know / No answer
Clearly assigned competent national authorities or bodies as established by Member States for supervising the systems put in place by online platforms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cooperation mechanism within Member States across different competent authorities responsible for the systematic supervision of online platforms and sectorial issues (e.g.						

consumer protection, market surveillance, data protection, media regulators, anti-discrimination agencies, equality bodies, law enforcement authorities etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cooperation mechanism with swift procedures and assistance across national competent authorities across Member States	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Coordination and technical assistance at EU level	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
An EU-level authority	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cooperation schemes with third parties such as civil society organisations and academics for specific inquiries and oversight	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other: please specify in the text box below	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

### 3 Please explain

*5000 character(s) maximum*

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

*3000 character(s) maximum*

### 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*

### 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*

Enforcement of advertising regulations (prohibited advertising content, advertising labelling) and enforcement of youth protection provisions of the Audiovisual Media Services Directive.

### 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 \(https://ec.europa.eu/digital-single-market/en/digital-services-act-package \)](https://ec.europa.eu/digital-single-market/en/digital-services-act-package)

## Background Documents

[\(BG\) Речник на термините](#)

[\(CS\) Glosř](#)

[\(DA\) Ordliste](#)

[\(DE\) Glossar](#)

[\(EL\) á](#)

[\(EN\) 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

