

# Digital Services Act package: open public consultation

Fields marked with \* are mandatory.

## Introduction

---

The Commission recently [announced](#) a Digital Services Act package with two main pillars:

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

**T h i s**

**c o n s u l t a t i o n**

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

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

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

**Digital services and other terms used in the questionnaire**

The questionnaire refers to **digital services** (or 'information society services', within the meaning of the E-Commerce Directive), as 'services provided through electronic means, at a distance, at the request of the user'. It also refers more narrowly to a subset of digital services here termed **online intermediary services**. By this we mean services such as internet access providers, cloud services, online platforms, messaging services, etc., i.e. services that generally transport or intermediate content, goods or services made available by third parties. Parts of the questionnaire specifically focus on **online platforms** – such as e-commerce marketplaces, search engines, app stores, online travel and accommodation platforms or mobility platforms and other collaborative economy platforms, etc.

Other terms and other technical concepts are explained in [a glossary](#).

## H o w t o r e s p o n d

Make sure to **save your draft** regularly as you fill in the questionnaire. You can break off and return to finish it at any time. At the end, you will also be able to upload a document or add other issues not covered in detail in the questionnaire.

## D e a d l i n e f o r r e s p o n s e s

8 S e p t e m b e r 2 0 2 0 .

## L a n g u a g e s

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

## About you

---

### \* 1 Language of my contribution

- Bulgarian
- Croatian
- Czech
- Danish
- Dutch
- English
- Estonian
- Finnish

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

\* 2 I am giving my contribution as

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

\* 3 First name

Miika

\* 4 Surname

Blinn

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

miika.blinn@vzbv.de

\* 7 Organisation name

*255 character(s) maximum*

Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)

\* 8 Organisation size

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

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.

2893800753-48

## \* 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                         |
| <input type="radio"/> Austria             | <input type="radio"/> Finland            | <input type="radio"/> Mauritius        | <input type="radio"/> Slovenia                         |
| <input type="radio"/> Azerbaijan          | <input type="radio"/> France             | <input type="radio"/> Mayotte          | <input type="radio"/> Solomon Islands                  |
| <input type="radio"/> Bahamas             | <input type="radio"/> French Guiana      | <input type="radio"/> Mexico           | <input type="radio"/> Somalia                          |
| <input type="radio"/> Bahrain             | <input type="radio"/> French Polynesia   | <input type="radio"/> Micronesia       | <input type="radio"/> South Africa                     |

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

- 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
- Cyprus
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Latvia
- 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
- Saint Barthélemy
- 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
- 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*

The regional consumer advice centres in Germany frequently receive consumer complaints on fake and counterfeit goods as well as non-conforming products that have been bought on online marketplaces. These consumers especially report low-quality electronic goods, as non-conformity can easily be detected in these cases (i.e. through potentially dangerous electric shocks), high levels of chemicals, potentially dangerous parts in clothes etc which often can only be assessed by formal lab tests. The German test organisation, Stiftung Warentest, together with five other European consumer organisations, recently tested a number of products for safety and conformity with EU rules that bought on online marketplaces. In total, they

purchased 250 products on well-known marketplaces and checked their safety. They released the results this year: <https://www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html> Two-thirds of the products purchased have been found not to be compliant with EU product safety rules. Among the follow-up actions taken were: providing information to other consumer groups through the BEUC, ICRT and CI consumer groups' networks, informing market surveillance authorities and platforms at national level.

As Verbraucherzentrale Bundesverband does not conduct tests of consumer goods, we would like to highlight tests which have been recently concluded by other European consumer organisations on this matter.

- Stiftung Warentest special dossier on Unsafe children's toys purchased at Amazon (December 2018): <https://www.test.de/presse/pressemitteilungen/Sicherheit-von-Kinderprodukten-Jedes-vierte-Produkt-fuer-Kinder-ist-mangelhaft-5412651-0/>

Other Member States' consumer organisations have conducted similar research, as provided in BEUC's answer to this question. vzbv bases its deliberations on these studies and evidence as well.

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*

The experience of consumers greatly depends on the type of online platform in question. What constitutes illegal behaviour varies between platforms acting as online marketplaces and platforms acting as social media providers (henceforth referred to as “interaction platforms”). Since the question explicitly mentions illegal goods, vzbv will list experiences with online marketplaces and comparison platforms (henceforth referred to as “transaction platforms”), as opposed to interaction platforms.

vzbv tried to find out how one could report illegal products to online platforms but had to give up since no easily accessible information was found – at least on Amazon and AliExpress (both signatories of the “Safety Pledge”).

A problem German consumers often report to vzbv and its regional consumer advice centres is that after having bought an item via an online marketplace, it is very difficult to report a problem to a foreign trader. Often the online marketplace is not cooperative or responsive and consumers do not receive any feedback, or they are given the contact details of their contractual partner who does not communicate properly.

Also, consumers reported to vzbv that in case of complaints, their user account got blocked or they were offered a discount under the condition that they drop the complaint. In that respect consumers are often lost between the platform and the (foreign) seller when they want to report a problem or non-conforming good.

The German consumer organisation Stiftung Warentest also recently tested reviews on online marketplaces and demonstrated how easy it is to mislead consumers through fake reviews that are not detected by the marketplaces most of the time (<https://www.test.de/Fake-Bewertungen-Wie-Verkaeuer-mit-gekauftem-Lob-Kunden-manipulieren-5401497-5624942/>).

At the moment, transaction platforms provide buying opportunities through their online distribution channel, but offer little control or enforcement when something goes wrong. At the same time, the transaction platform is in many cases the main beneficiary of the contract concluded. All in all, this leads to the consumer being bound to the platform as a customer, but the fulfilment of the contract is carried out by a third party who – in most cases - is widely unknown and intangible for the consumer. Such a distribution of responsibility is foreign to German and European contract law and must not lead to a disadvantage for consumers. EU product liability and product safety rules, as well as legal guarantees and the consumer’s right of withdrawal must not be undermined just because the seller is from a third country. If a supplier cannot be reached for a visual inspection of the goods, for complaints or to be confronted with liability claims, transaction platforms must assume liability instead of the trader. The platform may free itself from the liability if it can prove that it has sufficiently verified the supplier in question and its compliance with EU law

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

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

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

*5000 character(s) maximum*

The COVID-19 outbreak resulted in major disruption to people's daily lives, travels and finances.

vzbv and other German consumer organisations continuously advised consumers on the best way forward and collected information about additional difficulties arising during the pandemic.

See <https://www.verbraucherzentrale.de/marktbeobachtung/coronaaerger-wir-brauchen-ihre-hinweise-48369>

When addressing good practices (and problems) of online platforms in the wake of the COVID-19 outbreak it is important to keep in mind the distinction between transaction platforms and interaction platforms. What constitutes good practice or negligence must be assessed keeping in mind the social, legal and financial role of the respective platform.

The collected data shows that, with regard to online purchases from transaction platforms, it has often been difficult for consumers during the pandemic to hold transaction platforms or traders on the platform liable in case of problems. Many consumers report that they have been referred back and forth between trader, platform and payment service, with none of the companies assuming responsibility or meeting their obligations. This reinforces vzbv's finding that transaction platforms must assume a higher degree of responsibility for contracts concluded on them.

In addition to activities of European consumer organisations, vzbv welcomes as a best practice that in the joint Commission-EEAS Communication on tackling COVID-19 disinformation – Getting the facts right”, there is a commitment to further finance authorities “to do agile monitoring of markets” and a vision to provide an appropriate common enforcement toolbox for authorities. Joint market surveillance actions at EU level, like the CASP 2020 on COVID19 protective equipment should continue to be supported in the future, with ideally shorter timelines between the testing phase and the release of results/follow-up actions by authorities.

This shows that on top of flagging best practices, COVID-19 reinforced previous findings particularly for some goods and practices (e.g. price gouging, fake reviews, scams) and increased the scale of the problem as many more consumers turned to e-commerce sites and applications to shop. See, for example reports from

- UFC-Que Choisir : <https://www.quechoisir.org/actualite-coronavirus-hausse-du-prix-des-imprimantes-n77775/>

- Which?: eBay and Amazon failing to prevent sellers profiteering during coronavirus crisis <https://www.which.co.uk/news/2020/03/online-marketplaces-coronavirus-update-ebay-and-amazon/>

- Which?: Price-gouging still rife on marketplaces amidst coronavirus <https://www.which.co.uk/news/2020/04/price-gouging-still-rife-on-marketplaces-amidst-coronavirus/>

- Which? reported a “spike in fake Facebook ads selling rip-off clothing during coronavirus pandemic. The increase in the number of counterfeit goods being sold off the back of the coronavirus crisis is frightening” <https://www.thesun.co.uk/money/12086938/fake-facebook-adverts-rip-off-clothes/>

## 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*

Reporting mechanisms and follow-ups are not always clear, consistent, fully transparent or accountable to third parties such as consumer organisations or competent authorities. The DSA must change that and introduce clear obligations on this point, e.g. rules for platform design like for example: easily recognisable procedures, straightforward online contact and immediate possibility of communication. Furthermore, it must be ensured that users are able to get in "legal" contact with platforms with reasonable effort. It is thus advisable to make it mandatory for the platform to name a domestic authorised correspondence recipient (like for example in the German Netzwerkdurchsetzungsgesetz (NetzDG) § 5).

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*

Concerning transaction platforms, Stiftung Warentest found that Google stopped the uploading of new reviews during the pandemic allegedly due to staff shortages (Stiftung Warentest suspects that the real reason could be to stop bad reviews). Reviews became possible again after the end of the confinement. In addition, Stiftung Warentest acted as fake reviewers and buyers of fake reviews undercover. They obtained very worrisome insights from the practices of the companies that sell fake reviews. For example, some agencies gave them tips on how to avoid being discovered by the Amazon algorithm (e.g. by uploading only one or two reviews per week). The agencies also said they can purchase top ratings without problems for any of the products sold through their website. See the full story at <https://www.test.de/Fake-Bewertungen-Wie-Verkaeufer-mit-gekauftem-Lob-Kunden-manipulieren-5401497-5624942/>

Concerning interaction platforms there have recently been worrying reports. Due to the pandemic, interaction platforms had to send content moderators home. To compensate for this, youtube for example has relied more heavily on automated filters. This led to twice as many videos being taken down in the second quarter of 2020 as the first. This resulted in an openly admitted decreasing level of accuracy and shows the shortcomings of automated filter systems. One consequence of this is that you silence users who have done nothing wrong. See the full story at <https://www.protocol.com/youtube-content-moderation-covid-19>

With this evidence, digital services providers must take measures to prevent things like this. They cannot wait for specific reporting arguing they did not have “actual knowledge” of a specific issue.

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*

We refer to our response in question 10.

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*

With regards to scams and other unfair commercial practices, we refer to the research highlighted above. In addition, we recall that other platforms like Booking.com were found to infringe EU consumer law and had until 16 June 2020 to make significant changes to stop unfair practices, including misleading information about rebates, misleading representation of prices, and undue pushing of consumers: [https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/coordinated-actions\\_en](https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/coordinated-actions_en)

Overall, the focus seems to be put on a reactive approach. Platforms seem to wait for notices, for filters to catch something or for political pressure or public outcries. We encourage the European Commission to also look at platforms' business model as clickbait-led and data hungry business models are leading to the online spread of illegal activities. vzbv encourages the Commission to also look at a "better platform design" approach. Platforms should have duty to design their platform favourably towards consumers. Here, transparency obligations would not be enough. The Commission can take inspiration from Cobbe, Jennifer and Singh, Jatinder, "Regulating Recommending: Motivations, Considerations, and Principles" (April 15, 2019). (2019) European Journal of Law and Technology, 10(3), Available at SSRN: <https://ssrn.com/abstract=3371830>

21 Do you consider these measures appropriate?

- Yes
- No
- I don't know

22 Please explain.

*3000 character(s) maximum*

We recognise the efforts made by some platforms when they receive pressure, but research and evidence gathered shows it is not enough. Ultimately, it very much depends on their business model. Some unfair commercial practices (e.g. dark patterns or fake reviews promoted by traders) are fuelled by the business model of the platform. Their websites and/or apps are often not designed for checks and balances or legal compliance, but to capture attention and exploit consumers' behaviour and vulnerabilities. The DSA should be innovative and ambitious in tackling content optimisation, and the surveillance advertising business model.

## **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*



Not always. There are no harmonised procedures or clear duties on the actions that platforms are obliged to take. Stiftung Warentest showed that it is very easy and quick to create fake accounts or conduct illegal activities on platforms.

<https://www.test.de/Fake-Bewertungen-Wie-Verkaeufer-mit-gekauftem-Lob-Kunden-manipulieren-5401497-5624942/>

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*

No, consumers do not receive appropriate information. However, it is not only a matter of transparency but also about the design of the platforms themselves. Examples: it is not easy to distinguish an ad from a regular post on Instagram. In addition, when you check "stories" of your contacts, ads appear out of the blue. You can be informed about sponsored ads after three clicks, but consumers' choice is limited. For more details, see our responses to the section related to advertising and recommender 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*

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 type="radio"/>            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input checked="" type="radio"/> |
| To protect freedom of expression online, diverse voices should be heard   | <input type="radio"/>            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input checked="" 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 type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/>            |

### 3 Please explain.

*3000 character(s) maximum*

We would like to clarify that vzbv's scope of work does not focus on freedom of expression, but rather consumer protection, which is embedded in Article 38 of the Charter of Fundamental Rights. Hence why we respond to some answers "no reply".

It is important to point out that "disinformation" is not illegal in all circumstances or EU countries. The Digital Services Act should follow a rule of law approach. Disinformation is a symptom of a broader problem, that is, the business model.

As the EDPS put it, the EU has "focused on transparency measures, exposing the source of information while neglecting the accountability of players in the ecosystem who profit from harmful behaviour". "Online manipulation is also a symptom of the opacity and lack of accountability in the digital ecosystem". Cf.

[https://edps.europa.eu/sites/edp/files/publication/18-03-19\\_online\\_manipulation\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf)

In this sense vzbv welcomes that the Commission included in their inception impact assessment for the DSA the commitment to explore online advertising and commercial communications, including political advertising and micro-targeting aspects. This is also in line with the initial draft report from the JURI Committee in the European Parliament.

### 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*

We refer to our response to previous questions.

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

*3000 character(s) maximum*

We refer to our responses to previous related questions.

### **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*

We are not aware of this happening in the product safety area because for the moment the removals that Member States request are based on Safety Gate notifications which means they have indications that there is a serious risk for consumers (and often they have laboratory test reports available to prove this). We are also not aware of examples or the scale of erroneous removals based on consumer law violations. We are aware of errors happening with regards to copyrighted content. See for instance <https://juliareda.eu/2017/09/when-filters-fail/>. It is important to understand that this goes beyond mere anecdotal knowledge. Empirical evidence of over-removal can be found here <http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws>

---

***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*

According to the voluntary “Product Safety Pledge”, most big online marketplaces signed with the European Commission, platforms should “provide a clear way for customers to notify dangerous product listings”. vzbv research, however, showed that such a “clear way” is not to be found on platforms like Amazon or Aliexpress.

Also, sometimes even products that were listed on RAPEX/Safety Gate were up for sale (<https://www.which.co.uk/news/2019/11/dangerous-toys-and-killer-car-seats-listed-for-sale-at-marketplaces-like-amazon-and-ebay/#Dangeroustoy>).

In other cases, products that had been flagged for being dangerous and/or illegal reappeared quickly again after having been removed (<https://www.which.co.uk/news/2019/11/dangerous-toys-and-killer-car-seats-listed-for-sale-at-marketplaces-like-amazon-and-ebay/#Recalledtoy>).

Transaction platforms also react differently as to their respective jurisdiction: in the US, Amazon banned the sale of some child school materials and children jewellery unless sellers had valid lab testing or other proof of these not being toxic: <https://www.atg.wa.gov/news/news-releases/ag-ferguson-amazon-must-remove-toxic-school-supplies-kid-s-jewelry-marketplace>. The UK consumer organisation Which? reported that Amazon also launched a chemicals policy in the US as part of its Code for suppliers, but this has not been done for its UK Code: <https://www.which.co.uk/policy/consumers/5234/onlinemarketplaces>

In some cases, consumer organisations do not get appropriate or timely responses. This has for example happened to Forbrugerrådet TÆNK regarding unsafe cosmetics sold on wish.com: <https://kemi.taenk.dk/bliv-groennere/wishcom-hvad-er-der-mon-i-produkterne>

We also do not have information about the number of consumers that had bought the illegal products on online marketplaces and whether product recalls are carried out. Not all platforms commit to carry out those recalls themselves. Some platforms inform sellers about it (e.g. eBay: <https://www.which.co.uk/news/2019/02/why-are-ebay-and-amazon-still-selling-killer-car-seats/>) but it is unclear what actions sellers have taken. Platforms do not share such follow-up information with consumer organisations. We do not even know with certainty whether they collect such information.

Finally, consumers reported problems to contact some platforms in case of problems. All digital service providers should be obliged to put forward an easy-to-find and user-friendly mechanism for reporting problems, also for consumers. Redirecting to a general customer service address, chat bot or a phone number is not sufficient. Most consumers would give up as they are not encouraged to notify of possible wrongdoings.

Faced with extensive room for improvement, the DSA must put forward clear, procedural, conduct and transparency obligations for digital services to address these issues, putting the consumer interest first.

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

*3000 character(s) maximum*

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

*3000 character(s) maximum*

In the past years, vzbv and the German consumer advice centres have received a rising number of consumer complaints regarding online marketplaces or sellers that are not established in the EU. The complaints were addressed both to online marketplaces established in the EU linking to third country sellers (e.g. Ebay or Amazon) and to marketplaces that are not established in the EU (notably Wish, Joom, Floriday, Aliexpress and Shein). Next to complaining about dangerous electronic products, consumers mostly had their rights of withdrawal and legal guarantees breached and lacked information about their contractual partner or the contact information of the former. In that respect, vzbv published consumer warnings as to shopping on third country marketplaces

(<https://www.vzbv.de/pressemitteilung/billig-kleidung-aus-asien-marktwaechter-raten-zur-vorsicht-beim-online-shopping>; <https://www.vzbv.de/pressemitteilung/marktwaechterwarnung-kontaktsperre-fuer-wish-kunden>).

BEUC-vzbv research ([https://www.beuc.eu/publications/beuc-x-2017-122\\_the\\_challenge\\_of\\_protecting\\_eu\\_consumers\\_in\\_global\\_online\\_markets.pdf](https://www.beuc.eu/publications/beuc-x-2017-122_the_challenge_of_protecting_eu_consumers_in_global_online_markets.pdf)) however has shown that very often, consumers do not even realise that they are buying from foreign traders. Information on the websites about the seller is usually hard to find or presented in a user-unfriendly, intransparent or unclear manner.

There are also other problems that are not safety-related but infringe EU consumer law, such as the difficult enforcement of guarantee rights or issues with after-sales services. In order to enforce consumer rights also regarding online-marketplaces and foreign traders, vzbv regularly enforces consumer rights vis-à-vis traders that are established in third countries. However, especially regarding traders established in China and Hong Kong, this has not proven successful so far.

While consumers are bound to the platform, the contract fulfilment is carried out by a third party who – in many cases – is unknown and unreachable for the consumer. EU product liability and product safety rules, as well as legal guarantees and the right of withdrawal must not be undermined just because the seller is from a third country. If a supplier cannot be reached for complaints, liability claims or for a visual inspection, transaction platforms must assume liability instead of the trader. The platform may free itself if it can prove that it has sufficiently verified the supplier in question (see also answer 2.7 for more detail).

To solve this, we inter alia ask the Commission to review the General Product Safety Directive; include within the scope of the DSA a strengthening of platform liability (for transaction platforms) with regard to providers established in third countries and establish appropriate enforcement mechanisms of EU rules; and strengthen international cooperation.

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

1000 characters are not enough to put all relevant links. Please refer to the selection of Links in the feedback to this consultation of BEUC, which bundles its member organisations' evidence in one Document. We have flagged this to various Commission services.

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

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

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

3000 character(s) maximum

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

- Yes
- No
- I don't know

13 How valuable is this information for you?

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



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

*3000 character(s) maximum*

---

*The following questions are targeted at online intermediaries.*

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

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

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

2 Please explain.

*5000 character(s) maximum*

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 type="radio"/>   | <input type="radio"/>                | <input type="radio"/>   | <input checked="" type="radio"/>            |
| Detect illegal content, goods or services  | <input type="radio"/>   | <input type="radio"/>                | <input checked="" type="radio"/>  | <input type="radio"/>                       |
| In particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law | <input 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*

Overall, regardless of size, companies need to ensure a high level of consumer protection. It would be both inappropriate and misleading for consumers to create a two-tier system depending on whether a firm is big or small. However, enforcement can be adapted to size. Ex-ante measures for gatekeeping platforms, competition law and the new competition tipping tool under consideration can address some of the concerns for start-ups and SMEs.

Specific comments:

- It is unclear what the Commission means by "maintaining a system for assessing the risk of exposure to illegal goods or content". We need more clarity about what is meant to show support or not.

- Trusted flaggers: if there is anyone that deserves fast analysis and response is competent authorities. Resorting to trusted flaggers can shift responsibility from platforms to third parties. Trusted flaggers can sometimes be questionable – see for example <https://www.youtube.com/watch?v=xT9BRUoXhh8> (as of 4' 47").

Handling notifications by other parties cannot be discriminated or delayed. If this mechanism was to be part of the DSA, we need a framework for transparency, accountability and oversight for trusted flaggers.

- Detection of illegal content, goods or services: Recognising the difference between interaction platforms and transaction platforms, there is no one answer to this question. For transaction platforms, vzbv expects that such detection will be carried out using automated tools to detect illegal activities online (filters). For interaction platforms (e.g. social media platforms), vzbv opposes mandatory filters, as there is evidence they

do not properly work and can have counterproductive effects, particularly when dealing with user-generated content. In the case of transaction platforms (online marketplaces and comparison websites) however, consumers can suffer direct economic damage or even damage to their health in the course of contract execution. These risks justify the introduction of clear responsibility and liability rules for transaction platforms. In response, platforms will in some places have to detect and remove illegal goods or services.

- Informing professional users of compliance with the law: Informing of the law is not an effective solution to the issues we see, particularly marketplaces. We see some platforms already do that. More importantly, transaction platforms need to be liable for business users' EU law violations on the platform, if the platform fails to take appropriate measures. There are also issues with marketplaces notifying sellers about recalls as often, no information is provided about whether sellers have carried them out.

- Know your customer principle: It's not about mere identification (there are already obligations to gather certain data under both the e-Commerce Directive, consumer law...), but about robust verification, especially with regard to transaction platforms. To reduce the appearance of online illegal activities in the first place, transaction platforms should additionally make sure that sellers can be held liable for adherence to EU consumer law and cannot dodge responsibilities e.g. by switching accounts or simply not answering. An effective reporting system needs to be implemented, and sellers who, according to data available to the platform, appear to be unresponsive to claims must immediately be removed from the platform.

- Transparency about content policies, measures and their effects: More transparency is needed, particularly on advertising and rankings. However, we won't solve everything with transparency. We need rules of conduct and concrete obligations for platforms to design their platforms with consumer interests in mind, not only profit.

- Other measures: the root of the problem of illegal activities lies on the business model of platforms. They must be responsible for how they curate/optimize/rank/present content, services and products. vzbv asks for:

1) Transparency leading to user agency. This notably includes auditability of algorithms by authorities but also by independent third parties, such as consumer organisations. On top of transparency, we need rules of conduct for content curation/optimisation, rankings included.

2) The EU should also ensure opt-in requirements into algorithmic recommender systems (e.g. the Youtube auto-play should be an opt-in feature, not be on by default) and right to object to AI-based content curation or optimisation.

These recommendations would complement our efforts on the (hopefully) forthcoming ePrivacy Regulation which, ideally, should only allow tracking of electronic communications with consumers' informed, unequivocal, unambiguous consent. They would also complement existing rules in the Omnibus Directive and the P2B Regulation.

See the included vzbv's position paper on the DSA for other obligations to consider.

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*

vzbv advocates for setting up notice and action principles, taking into account differences regarding the type of online illegal activity at hand. For complex areas of law like copyright, a notice-and-notice system will be more appropriate. For illegal products, swift and effective action is needed.

We need requirements for targeted actions, a notice format, validity of notices, expeditious action and safeguards. The system needs to be easily accessible, user-friendly, not posing obstacles to seek redress or alert illegal activities. See our attached position paper for further details.

With regards to the precise reason for activities to be considered illegal, it is important to differentiate between consumers and professional business users (e.g. notices from specialised agencies for rightholders). For consumers, we should not set a too burdensome standard that cannot be fulfilled by them. Consumers can sense something does not seem right and should be able to explain why the activity is illegal but may not be able to be as precise as pointing out a specific law violation. When it comes to business users, our standards must be higher. We have to take into consideration that a majority of notifications today are sent by robots, not humans. Especially in such constellations, measures against the misuse of reporting systems (e.g. too many false claims) must be considered. Like for example an exclusion from the noticing system. For the user, on the other hand, it is important to implement an obligation for the platform to easily restore his or her content (put back obligation) in the case of false allegations.

Another problem we would like the DSA to solve is that most platforms often remove online activities on the basis of their terms and conditions, not the law. The DSA should ensure a rule of law approach by requiring platforms to apply corresponding legislation to the notice received by third parties.

#### 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*

Some platforms use technology to detect activities that can be illegal (or, better said, that are against their terms of service). Experience has shown that automated tools or filters may help, but do not really tackle the issue. For example, when some BEUC members report about the sale of some unsafe products, some platforms' PR points are to say they invest in human resources and filters to detect them, but that "bad actors" will always try to bypass their system.

See for example: <https://www.which.co.uk/news/2019/02/why-are-ebay-and-amazon-still-selling-killer-car-seats/>

This answer is not satisfactory, particularly when dangerous products keep reappearing.

We encourage the Commission to focus on measures to reduce the scale of the problem: tackle dangerous business models (notably based on clickbait and data hungry options), have robust obligations to verify traders, have obligations to do random checks on services and products facilitated via their platforms; and put forward a strong, effective and resourceful enforcement. A specific liability regime should also be introduced for certain types of platforms, namely marketplaces, to ensure they can be held liable if they fail to fulfil their duties. Vzbv believes that in principle, liability should rest with the seller, not the platform. But the platforms must be required to help enforcing EU consumer law and, if they fail to do so, must be held liable just as the seller would. These measures won't eliminate reappearance of illegal activities 100%, but if applied and enforced properly, they should significantly reduce the number of illegal activities online. What is clear is that we cannot simply wait for a notice and action system.

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 consequences and effects may vary. When it comes to content, a lot depends on contextualisation. It is well known about the inaccuracy of these tools. This is also finally openly admitted by the German government ([https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/DiskE\\_II\\_Anpassung%20Urheberrecht\\_digitaler\\_Binnenmarkt\\_FAQ.pdf?\\_\\_blob=publicationFile&v=1](https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/DiskE_II_Anpassung%20Urheberrecht_digitaler_Binnenmarkt_FAQ.pdf?__blob=publicationFile&v=1)) and the European Commission as well. In the current copyright stakeholder dialogue, the European Commission wrote in their published draft for the guidance: "It should be born in mind that in the current state of the art, content recognition technology cannot assess whether the uploaded content is infringing or covered by a legitimate use." <https://ec.europa.eu/eusurvey/runner/4fd43123-6008-a214-f572-4ecd331b9e0e>

Similar outcome when it comes to review mechanisms. For example, when Which? spotted that eBay's business model and review mechanism is misleading consumers into buying shoddy products, eBay said that they use filters: <https://press.which.co.uk/whichpressreleases/flawed-ebay-review-system-dupes-consumers-into-buying-shoddy-products/>

We need to move beyond conversations we had already in the context of the copyright Directive. As per the previous answer, we need effective solutions. Technology is not proven to be accurate, effective or sufficient. At least we need a user-friendly deployment of technology. For Interaction Platforms this means in concrete terms that the following parameters should be taken into account in particular in the decision to restrict or delete content in line with the principle of proportionality:

1. the identity of the person behind the notice;
2. the identity of the user;
3. the user's own assessment regarding the content (pre-flagging);
4. the time-critical nature of the content, and
5. the harmful potential of the content.

Finally the user affected by a complaint should be given the right to comment on the decision before the content is taken down (stay up obligation, delayed takedown). This is a necessary specification of the notice and action procedure. It will ensure that content can only be taken down after a comprehensive review, which includes obtaining the opinion of the uploader.

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*

On the one hand, the territorial scope should cover all entities that provide services, products and/or digital content to EU consumers, regardless of them having an establishment in the EU. This can mirror Article 3 and recital 23 of the General Data Protection Regulation (GDPR). Currently, the e-Commerce Directive establishes that it should not apply to providers established in third countries (recital 58). This is a well-recognised loophole that must be addressed in the DSA.

The DSA needs to ensure that transaction platforms properly check the sellers listed on their platform, especially those that do not dispose of a legal entity in the EU. As the consumer is bound to the platform as a customer, but the fulfilment of the contract is carried out by a third party who – in many cases - is completely unknown and intangible to the consumer. Such a distribution of responsibility is foreign to German and European contract law and must not lead to a disadvantage for consumers. EU product liability and product safety rules, as well as legal guarantees and the right of withdrawal must not be undermined just because the seller is from a third country. If a supplier is not available for complaints, liability claims or for a visual inspection, transaction platforms must assume subsidiary liability for this. The platform may free itself if it can prove that it has sufficiently verified the supplier in question.

These due diligence obligations should at least encompass the following:

- The requirement that providers must identify themselves personally and only one registration per identification document is allowed.
- A procedure to ensure that providers cannot close and re-open their presence without obstacles.
- An easy way to report problems with a provider.
- A verification that providers are available and will settle legitimate claims in case of conflict.

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*

From a consumer perspective, vzbv is more concerned by services that communicate with/to the public. Services deeper in the internet stack should be resorted to as a last measure, after different means have been exhausted and in serious damaging scenarios. For example, to take down a domain name would be more disproportionate than tackling concrete illegal activities on a website via the hosting provider. Of course, if a whole website contains illegal activities and they cause serious detriment to consumers, authorities could request to take it down as a last resort. This is the approach taken under the Market Surveillance Regulation and the CPC Regulation.

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*

Interested third parties can indeed help platforms to better protect consumers online. Consumer organisations have shown great responsibility and taken resources to conduct tests, analyses and research on platform activities. The evidence is staggering. We would like to highlight that platforms are the consumer-facing company consumers interact with. We notice platforms have a tendency to shift responsibility emphasising that they cannot tackle illegal activities alone. While true, platforms' role should be stronger than the current one. For example, online platforms should have an obligation to report illegal content, services or goods (e.g. unsafe products being sold or promoted via their websites or apps) to competent authorities when they become aware of them, without prejudice to other applicable EU laws. Tackling illegal activities goes beyond removals and waiting for notices from third parties.

With regards to authorities, vzbv recommends:

- Out-of-silos cooperation between authorities, for example between data protection, consumer protection and competition authorities; and between market surveillance and customs authorities. This can be based on Article 6 of the CPC Regulation. A network of national central authorities can be established with an obligation to cooperate with, seek advice from and to not interfere with other authorities' competences provided for by EU and national law.

- Better cross-border cooperation between authorities.

- Improved collaboration between authorities and civil society, including consumer organisations which can alert relevant authorities, e.g. referring evidence about the sale of dangerous products online via various platforms. We strongly recommend requesting authorities to respond to the alerts within a reasonable time.

- Introducing an obligation for Member States to grant adequate resources for authorities. For example, one million parcels arrive per day at Liège's airport. As Alibaba will open a warehouse there in 2021, the airport expects this figure to go as high as 7 million per day by then. This is a challenge for customs and market surveillance authorities. They will need adequate resources. Other horizontal laws like the GDPR have introduced this requirement.

- The revised market surveillance Regulation (2019/1020) which will take effect on 16 July 2021 enables market surveillance authorities to conduct mystery shopping online. Member states need to ensure the authorities are granted adequate resources for this task.

**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*

vzbv advocates for a rule of law approach. vzbv advocates for legal certainty making problematic activities illegal. For example, when Which? reported about thousands hackable wireless cameras being sold on marketplaces, eBay stated the cameras were “legal to sell in the UK, and complied] with [eBay’s] existing policies.”

<https://press.which.co.uk/whichpressreleases/more-than-100000-hackable-cameras-in-uk-homes-warns-which/> This type of evidence shows the need for strengthening laws (in this case, cybersecurity and safety legislation). In addition, vzbv advocates for better platform design as the root of most problems in the platform economy lie on their business models and how information is presented to consumers. Ultimately, we need secondary liability of online marketplaces as an incentive not to sell such products.

vzbv is not against complementary voluntary measures e.g. to protect children or to protect consumers from scams. In grey areas, platforms should continue being able to engage with consumer organisations (e.g. like Which? has done) and take voluntary measures to protect consumers. For illegal activities, voluntary actions should not be promoted as they have proven to be ineffective, often non-transparent and unaccountable.

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

*5000 character(s) maximum*

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

|  | 1 (not at all necessary) | 2                     | 3 (neutral)           | 4                     | 5 (essential)                    | I don't know / No answer |
|--|--------------------------|-----------------------|-----------------------|-----------------------|----------------------------------|--------------------------|
| Transparently inform consumers about political advertising and sponsored content, in particular during election periods                    | <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 type="radio"/>            | <input checked="" type="radio"/> |
| Ensure effective access and visibility of a variety of authentic and professional journalistic sources   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/>            |
| Auditing systems for platform actions and risk assessments   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/>            |
| Regulatory oversight and auditing competence over platforms' actions and risk assessments, including on sufficient resources and staff, and responsible examination of metrics and capacities related to fake accounts and their impact on the manipulation and amplification of disinformation. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/>            |
| Other (please specify)   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/>            |

### 13 Please specify

*3000 character(s) maximum*

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

*3000 character(s) maximum*

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

|   | 1 (not at all necessary) | 2                     | 3 (neutral)           | 4                                | 5 (essential)                    | I don't know / No answer         |
|---|--------------------------|-----------------------|-----------------------|----------------------------------|----------------------------------|----------------------------------|
| High standards of transparency on their terms of service and removal decisions  | <input type="radio"/>    | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | <input 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 checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| Enabling third party insight – e.g. by academics – of main content moderation systems   | <input type="radio"/>    | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/>            |
| Other. Please specify   | <input type="radio"/>    | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input type="radio"/>            | <input checked="" type="radio"/> |

## 16 Please explain.

*3000 character(s) maximum*

With regards to assessing freedom of expression implications, vzbv recommends not to confuse rules for user-generated content with commercial activities such as the sale of goods (e.g. via an ad) or offering services (e.g. a hotel room).

In addition we refer to our response in question 6. In particular, it should be considered to give the user (affected by a complaint) the right to comment on the decision before the content is taken down (stay up obligation, delayed takedown). This is a necessary specification of the notice and action procedure. It will ensure that content can only be taken down after a comprehensive review, which includes obtaining the opinion of the uploader.

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*

We highlight that consumer protection is a principle protected under the EU Charter of Fundamental Rights (article 38). The DSA must ensure a high level of consumer protection. With regards to freedom to conduct business, we highlight that Article 16 of the Charter clearly sets forth that this freedom is provided within the limits of the law. Sometimes this freedom is misused or misquoted in policy discussions.

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*

We refer to our previous responses on these matters. We highlight again that more than the information provided, \*how\* it is provided matters most. Information obligations are not a panacea and will not solve the problems identified.

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*

As a matter of principle, online platforms should be transparent about the use of Algorithm-based Decision Making (ADM) systems with their users. Consumers should be firstly able to know if algorithms were used in order to take decisions affecting them such as in the mentioned activities. This should also be provided in addition to the legal obligations under the GDPR and regardless on whether data processed are to be considered as 'personal data'.

In addition, users should be also able to understand what the reasoning behind the automated system is and how it could impact their activities. For example, research shows many consumers do not understand how Facebook's news feed works. See <http://www.pewresearch.org/fact-tank/2018/09/05/many-facebook-users-dont-understand-how-the-sites-news-feed-works> The Omnibus Directive and the P2B Regulation offered some partial solutions. The DSA should complement them but do not fall into the "transparency fallacy". See in this regard Cobbe, Jennifer and Singh, Jatinder, "Regulating Recommending: Motivations, Considerations, and Principles" (April 15, 2019). (2019) European Journal of Law and Technology, 10(3), Available at SSRN: <https://ssrn.com/abstract=3371830>. For example, these researchers recommend companies to have "logs of recommended content (both for personalisation and for behavioural targeting) so that they can be reviewed by users and by oversight bodies".

Authorities should be able to test and certify that the systems being used are compliant with existing rules, also via testing the systems. To this end, authorities should be informed about the existence of ADM systems and should be put in condition to exercise corrective powers such as blocking illegal activities. It is therefore key that platforms use open interfaces allowing the competent authorities to intervene when needed.

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

*5000 character(s) maximum*



The EU should also ensure opt-in requirements into algorithmic recommender systems (e.g. the Youtube auto-play should be an opt-in feature, not be on by default) and the right to object to AI-based content curation or optimisation.

These recommendations would complement the EU efforts on the forthcoming ePrivacy Regulation which, ideally, should only allow tracking of electronic communications with consumers' (informed, unequivocal, unambiguous consent). They would also complement existing rules in the Omnibus Directive, the P2B Regulation and hopefully forthcoming regulation on AI.

The use of algorithmic systems for personalisation of contents by platforms raises some important concerns from a consumer's standpoint. Personalisation of products and services is nowadays very common in the online landscape and platforms should reflect this massive use in their policies. Therefore, a first key obligation for platforms should be to inform users transparently and satisfactorily about the way in which algorithmic systems select and filter the content they interact with. In this sense, platforms should be able to intelligibly communicate whether – for example - systems operate by using single input (like music) or multiple inputs within and across various platforms (i.e. news, sites and search engines).

As also stated in our latest position paper on AI [https://www.beuc.eu/publications/beuc-x-2020-049\\_response\\_to\\_the\\_ecs\\_white\\_paper\\_on\\_artificial\\_intelligence.pdf](https://www.beuc.eu/publications/beuc-x-2020-049_response_to_the_ecs_white_paper_on_artificial_intelligence.pdf) , the personalisation of content raises questions also in term of price-discrimination between consumers and group of consumers.

In this sense, we highlight that there should be no price discrimination by means of personalised and non-personalised automated assessments. Moreover, it is important to bear in mind that such services are often provided 'for free' in order to maximise the number of users and therefore the amounts of profit-generating consumer data collected for AI and ADM systems. This creates often an imbalanced relation between platform and users which should be normalised by – for example – empowering consumers with new and specific rights such as the right to object to automated processing.

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

The benefits would be to have real accountability, supervision and oversight. Currently, we are stuck with what platforms tell us they do. There is no comprehensive way to verify that what they say is true. Even transparency reports are often inconsistent and not comprehensive. We are aware that data protection is sometimes invoked by some companies not to share information to be held accountable. GDPR cannot be an excuse not to bring accountability and transparency to the platform. This point has been emphasised by the EDPS in its preliminary opinion on data protection and scientific research. “There is the suspicion of data protection being enlisted to escape accountability where, on the pretext of safeguarding the rights of others, inferred personal data is conflated with intellectual property, offering a shield for corporate secrecy”.

Cf. [https://edps.europa.eu/sites/edp/files/publication/20-01-06\\_opinion\\_research\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf)

## 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

Competent authorities must have the necessary enforcement tools to enforce the law. These include effective, proportionate and dissuasive sanctions. One clear incentive for platforms to comply with their obligations is to clarify when platforms – particularly online marketplaces – would be liable for damages, guarantees and contract performance issues when things go wrong.

Concerning over-removal of content one incentive could be that platforms bear the costs of their mistakes (e. g. small fees). Because suddenly over-removal also has a price tag, platforms have more incentive to improve. For more details: <https://balkin.blogspot.com/2019/06/why-there-is-no-due-process-online.html>

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

3000 character(s) maximum

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

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

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

The liability regime has been rather established under Member State law because the e-Commerce Directive has set forth liability exemptions and limitations for providers.

While vzbv recognises the benefits of the liability limitations for user-generated content on interaction platforms for facilitating and securing a forum for the free circulation of information and dialogue and for the freedom of expression, more clarity is needed for commercial content, services and products on transaction platforms. Just as the e-Commerce Directive has three articles differentiating liability provisions for mere conduit, caching and hosting services, we ask the European Commission to establish another article specific for online marketplaces, including platforms where suppliers can place advertisements, digital comparison or other advisory services, and platforms that offer reputation services, as well as hybrid platforms. We stress that Article 21 of the e-Commerce Directive states that when examining the adaptation of the Directive, the Commission should analyse *"the attribution of liability\* following the take down of content"* (emphasis added).

Nowadays, most hosting providers cannot claim they merely connect people. This is because they have the capacity to know and control information hosted or transmitted in their sites or apps. Platforms make money out of this intermediary function but also from their optimisation or curation. Therefore, clarification of the liability provisions in light of issues identified, market developments and case law is necessary.

When it comes to online intermediaries that facilitate the conclusion of a distance contract between consumers and other traders or consumers (i.e. they are online marketplaces), a special liability regime is needed.

In principle, the supplier on any given transaction platform should be liable for adherence to EU law. However, if a supplier is not available for complaints, liability claims or for a visual inspection, transaction platforms must assume secondary liability for this. The platform may free itself if it can prove that it has sufficiently verified the supplier in question. These due diligence obligations should at least encompass the following:

- The requirement that providers must identify themselves personally and only one registration per identification document is allowed.
- A procedure to ensure that providers cannot close and re-open their presence without obstacles.
- An easy way to report problems with a provider.
- A verification that providers are available and will settle legitimate claims in case of conflict.

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

### 3 Are there aspects that require further legal clarification?

*5000 character(s) maximum*

CJEU case law has to a certain extent clarified this question. The Commission can insert clarifications on that basis. What is clear is that “actual knowledge” cannot be the only standard to infer liability for online marketplaces. This is particularly relevant if the company has a predominant influence on the value chain. The European Law Institute proposed a non-exhaustive list of criteria to allow judges to determine predominant influence (See European Law Institute (2019) Model Rules on Online Platforms, Article 20, p. 19 [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)):

- a) “The supplier-customer contract is concluded exclusively through facilities provided on the platform;
- b) The platform operator withholds the identity of the supplier or contact details until after the conclusion of the supplier-customer contract;
- c) The platform operator exclusively uses payment systems which enable the platform operator to withhold payments made by the customer to the supplier;
- d) The terms of the supplier-customer contract are essentially determined by the platform operator;
- e) The price to be paid by the customer is set by the platform operator;
- f) The marketing is focused on the platform operator and not on suppliers; or
- g) The platform operator promises to monitor the conduct of suppliers and to enforce compliance with its standards beyond what is required by law.”

These criteria are inspired on the Uber Spain case c-434/15 (para. 39), where the CJEU ruled that “Uber exercises decisive influence over the conditions under which that service is provided by those drivers”; and in the Airbnb Ireland case c-390/18, where CJEU ruled Airbnb did not have decisive influence (para. 68).

In addition, they took inspiration from the Oberdorf v Amazon US Court of Appeals' ruling in Pennsylvania that held Amazon liable following the sale of a defective dog leash which left a consumer blind on an eye and the seller disappeared. Cf. <https://www2.ca3.uscourts.gov/opinarch/181041p.pdf> (the proceedings are still ongoing).

In case of a transaction platform exerting predominant influence over their supplier(s), the platform itself is the de-facto-supplier. It must be treated as such legally, and be liable for any violation of EU consumer law.

Finally, inspiration can also be drawn from the European Commission's Communication "A European Agenda for the collaborative Economy", which highlighted three criteria to determine the influence or control of platforms over the suppliers.

**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*

This question should rather be about whether the current legal system creates the right incentives for service providers – in particular platforms – to be held to account when things go wrong, e.g. when a consumer seeks damages /redress for a faulty product. The answer is “no” as the current regime does not clearly set up when platforms are liable (see response to question 2).

We would like to stress that the solution to current problems identified is not to expand liability protections, particularly with regards to self-regulatory measures. Some platforms have put up some mechanisms in place already (e.g. filters) to identify illegal or harmful activities. As previously explained and evidenced, they do not seem to be effective tools. Platforms do not need further protections, consumers do.

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*

Currently most of the platforms subject to public and private concern, including in case law, are considered as active providers.

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*

Article 15 of the e-Commerce Directive is still valid and appropriate, particularly to protect consumers' right to privacy. However, as mentioned earlier, the EU approach should not only focus on reactions to illegal activities, but also look at the business models, introduce a secondary liability system for platforms, impose random checks on products and services, facilitate sharing of data with authorities and third parties such as consumer organisations, strengthen enforcement and supervision, 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*

We very much support the Commission President's commitment to put forward a DSA to upgrade our liability and safety rules. As previously mentioned, this upgrade should notably be done by the creation of a specific article for online marketplaces, distinguishing them from other hosting providers (we refer to our response to previous questions). The notion of 'hosting service provider' is too broad. It needs some differentiation depending on the functionalities or services of companies. E.g. Facebook's purely social media service should be treated differently than the advertising service provided at the request of a (business) user.

### 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 type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/> |
| It is easy for consumers to switch between services provided by online platform companies and use same or similar services provider by other online platform companies ("multi-home").                            | <input type="radio"/>            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/> |
| It is easy for individuals to port their data in a useful manner to alternative service providers outside of an online platform.  | <input type="radio"/>            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input checked="" 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 checked="" type="radio"/> | <input 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 type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| When large online platform companies expand into such new activities, this often poses a risk of reducing innovation and deterring competition from smaller innovative market operators.    | <input type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

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

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

|  |   |
|--|---|
| Large user base  |  |
| 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*

The above criteria/concepts are too widely formulated. In relevant cases not all of these characteristics must be present.

The criteria should be used to identify a gatekeeper position for particular products/services or particular markets (e.g. the gatekeepers' core and adjacent markets). These criteria do not necessarily have to be cumulative in each case. The list of criteria must be reviewed regularly in order to ensure that the criteria reflect current market realities.

The following factors seem particularly relevant:

- Ability to exploit network effects.
- Ability to build and exploit "economies of scope" by combining various resources (e.g. data and access to users from different products/services, domains or markets/sectors).
- Ability to control access and determine conditions for consumers' access to a significant part of a market. (e.g. expressed in the ability to engage in tying and bundling of services and/or terms and conditions vis-à-vis consumers or business users.)
- Number of users and market share.
- Large scale accumulation of data relevant for a competitive advantage, leading to significant barriers to entry.
- Platforms in markets characterised by high and non-transitory barriers to entry.
- Exceptional ability to leverage assets (e.g. data) from one market to another.
- Lock-in effects on (business) users and consumers, the inability of consumers to multi-home and the presence of high switching-costs for consumers (i.e. costs for consumers associated with substituting the service/product/provider). (Degree of) Availability of an equivalent substitute for the service/product/provider.
- Asymmetrical bargaining power vis-a-vis business partners/competitors. E.g. the ability to control access and determine conditions for market participants of an ecosystem.
- Exceptional financial power or access to other resources.
- Vertical integration or activities on other related markets.

In addition to "They leverage their assets for entering new areas of activity" and "They build on and exploit strong network effects" there should be a category on "Economies of Scope":

Building up and exploiting "Economies of Scope" is different from leveraging resources from one sector to another as well as from "economies of scale". Economies of Scope, or "conglomerate Effects" refer to lowering average cost by producing more different types of products, making product diversification more efficient. E.g. Using data from consumer search queries in your core business can reduce costs for training AI-based digital assistants Models and vice versa. Thus, giving large, diversified conglomerate platform players an additional (cost) advantage fostering their positions in markets where they already established a presence, as well as facilitating leveraging their activities in adjacent markets.

### 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 criteria should be used to identify a gatekeeper position for particular products/services or particular markets (e.g. the gatekeepers' core and adjacent markets).

These criteria do not necessarily have to be cumulative in each case.

Regarding transaction platforms, gatekeeping power can additionally reach levels where it is no longer appropriate to classify the platform as an intermediary between supplier and customer. Online marketplaces in many cases exert intense control over trader and consumer behaviour on the platform. This control can amount to predominant influence where the platform itself is the de-facto-supplier and must be treated as such legally. Platforms can attain predominant influence e.g. by imposing strict and far-reaching terms and conditions, by maintaining control over the payment system, or by exclusively holding most consumer data and deciding which data is shared with suppliers.

The ELI's "Model Rules on Online Platforms" can also provide inspiration to the criteria of predominant influence. (See European Law Institute (2019) Model Rules on Online Platforms, Article 20, p. 19 [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))

### 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*

AI-based so-called smart digital assistants can be used to strengthen a gatekeeper position as they facilitate the build-up and exploitation of “conglomerate effects”/economies of scope: Digital assistants (e.g. Siri, Alexa etc.) communicate with consumers, assist them and collect consumer data in various of fields of life. E. g. Location, traffic navigation, consumption, smart home, health, entertainment, online search, speech /biometric data. Smart digital assistants increasingly occupy bottleneck positions in various markets: Acting as personalised recommendation systems they determine what products/services/items consumers choose from. Digital assistants can collect and analyse data form various domains of life and leverage them across adjacent markets.

Digital assistants constitute a bottleneck through which consumers access various markets. Vice versa they determine which products/suppliers get access to/are recommended to consumers.

## **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*

Unfair practices include:

- self-preferencing of own or linked services/products. Including Unfair terms and conditions consumers have to agree on, in order to get access to a significant part of a market or ecosystems.
- Intra-company sharing and Integration of consumer data obtained from different branches of a conglomerate firm or through different services
- Tying and bundling of services/and or terms and conditions vis-à-vis consumers.
- Limited control consumers have over their data including data mobility/data portability
- Use of pre-installation and defaults and of other nudging techniques.
- Exclusion of alternative, more consumer-friendly services of platforms/applications from ecosystems or platforms, thereby reducing consumer choice and hampering innovation as well as competition.

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*

See answer to question 9 above

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

*3000 character(s) maximum*

Hampering innovation and competition as well as reducing consumer choice and consumer welfare by preventing consumers to choose to form innovative, privacy-friendly alternatives.

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

*3000 character(s) maximum*

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

*3000 character(s) maximum*

Negative societal and economic effects include:

- Undermining consumer protection laws
- Undermining of data protection regulation
- Consumer self-determination: As more services and consumer data are controlled by larger economic entities, the larger is their ability to control what goods and services consumers get access to, e.g. by control of technical ecosystems or via recommender systems. As a result, there is the risk, that self-determination of consumers decreases.
- Limited consumer choice
- Further deterioration of consumers' bargaining power vis-à-vis enterprises
- Reduced contestability of market positions
- Reduced innovation

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

*3000 character(s) maximum*

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

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

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

## 2 Please explain

*3000 character(s) maximum*

Large gatekeeper platforms increasingly determine how consumer markets function. Some markets have become increasingly concentrated with a few large platforms acting as gatekeepers for many digital products and services accessed by consumers. While digital innovations increased consumer welfare over the past decades, these welfare gains become threatened in more recent times through excessive market concentration by gatekeepers for many digital products and services – especially if gatekeepers act across markets.

The reasons are underlying market characteristics that support and cement large platforms' market positions: lock-in and network effects, economies of scope and scale, as well as information asymmetries. Some online platforms have repeatedly been engaged in certain types of conduct (like self-preferencing, tying and bundling) and have thus reinforced this trend. This is facilitated as gatekeepers occupy central positions in a market or across markets – enabling them to set the rules of the game for suppliers and consumers alike, thereby acting in their own commercial interest. Transaction platforms that exert predominant influence over their suppliers dodge contractual responsibilities by hiding behind an intermediary role.

As a result, it becomes more and more difficult to ensure that digital markets remain fair and contestable for innovators, businesses, and new market entrants. This trend threatens to undermine the gains in consumer and social welfare that were generated by the digitised economy so far. This unfavourable development calls for policy-makers to take decisive actions at European level.

Considering the interplay of technology, data and economic power and the ability of platforms to leverage them across markets, the current European competition legislation is insufficient to address the challenges posed by gatekeeper platforms. There is the notion that the effectiveness of remedies in digital market cases solely through the enforcement of competition law as it currently stands is too limited. Although the enforcement of competition law has sanctioned and imposed remedies in individual cases, this has taken many years during which the harm to competition and consumers has persisted and sometimes increased.

The European Commission should design the Ex Ante Regulation and the envisaged New Competition Tool (NCT) in a complementary manner:

- a) A mix of general prohibitions/restrictions of certain unfair trading practices and targeted obligations for large online platforms acting as gatekeepers under the proposed Ex Ante Regulation envisaged in the DSA to tackle general problems.
- b) Specific tailor-made remedies for large gatekeeper platforms on a case-by-case basis under the NCT

to tackle structural competition problems.

Both, the Ex Ante Regulation and the NCT must also be complementary to the  
c) Existing enforcement of Articles 101 and 102 TFEU of anticompetitive conduct.

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*

The success of a policy approach based on an obligation/prohibition list depends on defining an unambiguous list of types of conduct which are broad enough in scope to catch all relevant conduct, but which is sufficiently precise to have the desired signalling effect to market participants and enable simple monitoring and enforcement.

The European Commission should consider supplementing the lists of prohibited practices and obligations with additional guidance notices. In order to ensure that the Ex Ante Regulation reflects current market characteristics and business practices it is essential that the European Commission regularly reviews and updates this list.

The following practices should be considered for inclusion in the list of prohibited/restricted practices:

- Prohibition of self-preferencing of own or linked services/products (e.g. in ad tech and search).
- Prohibition of restrictions of data portability beyond the GDPR.
- Deliberate product/service degradation on specific services channels in order to force consumers to agree to terms and conditions/install applications on their devices. E.g. deliberately reduced functionality of a map service on mobile phones web browsers in order to force consumers to install the platforms app (while the service fully functions with standard web browsers).
- Restrictions on using/integrating consumer data obtained from different branches of a conglomerate firm or through different services (for example where data has been collected through the leveraging of market power).
- Prohibition of practices of tying and bundling: In cases when gatekeepers sell a good or grant access to a service on the condition that the consumer uses/purchases a different service/product or agrees to terms and conditions that could be viewed as separate but are tied ("sold") together as a bundle. This includes cases where consumers want to get access to service and have to agree to use/install a different service or accept terms and conditions allowing the firm to collect and analyse more consumer data.
- Restrictions on gathering and/or use of data by gatekeepers from their business users to gain competitive advantage (to the extent necessary beyond the P2B Regulation).



- Restrictions on the use of pre-installation and defaults (in particular for browsers and search engines) and of other nudging techniques: imposing a “fairness-by-design” duty on gatekeepers to ensure that they make it as easy as possible for consumers to make genuine choices (rather than as presently, exploiting recognised consumer behavioural biases to channel/manipulate consumer choices and lock-in consumers).
- Restrictions on the exercise of bargaining power vis-a-vis trading partners in specified and, where relevant, to preclude gatekeepers’ use of unfair commercial practices vis-à-vis consumers.

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*

Obligations could be included where they can complement the prohibited/restricted practises set out above. These could include:

- Obligations to report specified relevant information to the EU Online Platform Observatory or the “Taskforce” (see next chapter) on particular activities on a regular basis.
- Obligation to support full effective data portability by consumers, including automated transfer of data to competitors upon consumers’ request.

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*

The primary principles underlying the proposed Ex Ante Regulation are competition related. Therefore, monitoring and enforcement could be performed by a new “Taskforce” led by DG COMP. At the same time, the Taskforce should also be responsible for the application of the case-by-case remedies envisaged in the New Competition Tool (NCT).

Depending on the specific issue at hand, the Taskforce should work in close cooperation with other Directorates-General , the data protection authorities as well as national enforcement bodies. Given the

inherent cross-border nature of platform conduct, the European Commission's Taskforce would take any necessary enforcement decisions with respect to the listed infringements of obligations or prohibitions under the DSA Ex Ante Regulation, unless another authority was better placed to do so in a particular case.

In enforcing the rules of the Ex Ante Regulation, the Taskforce could take account of infringements of the list of prohibited/restricted practises, unfair trading practices and competition-related issues not directly addressed by DG COMP under classic competition policy (e.g. cases enforced under Article 101 and 102 TFEU).

Benefits of the EU-Level Taskforce Approach:

- Due to its double role, the Taskforce is suited to avoid inconsistencies of application and enforcement between the Ex Ante Regulation and the NCT. This approach also maximises synergies by using NCT-findings to update the Ex Ante Regulation, making sure it reflects current market and business realities (e.g. in identifying gatekeepers subject to regulation and updating the list of prohibited practices).
- The risk of inconsistencies at Member State level enforcement and subsequent legal uncertainty would be avoided, while at the same time drawing on Member States competent authorities' expertise in specific cases /markets/issues.
- No major and lengthy (and thus harmful) institutional set up would be required to start enforcement, as the Taskforce could be put in place in a short timeframe.
- The Taskforce could call on existing experienced staff and could be operational immediately.
- Forum shopping by platforms would be prevented and maximum regulatory independence would be ensured.
- DG COMP is highly experienced in the types of procedures and processes required for analysis and enforcement of competition-related policies, including interim measures, evidentiary standards and respect for due process.
- The European Commission is best placed to easily facilitate EU-wide cooperation among the involved Member States authorities and with extra-EU jurisdictions, as large platform players often originate from outside the EU.

It would be essential for the Taskforce to be vested with appropriate legal powers (e.g. for carrying out investigation and enforcement) and endowed with sufficient financial, human and technical resources to carry out this new task.

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*

As set out under question 8, case-by-case remedies should be primarily dealt within the context of the “New Competition Tool” (NCT).

vzbv emphasis, that the interventions and remedies should be as open as possible in order to allow the competent authority as much flexibility as needed to deal with the peculiarities of each case.

The case-by-case remedies dealt within the context of the NCT should not be limited but applied in be flexible and open including structural and behavioural remedies. The remedies imposed could take inspiration from and should be consistent with Ex Ante Regulation (see above). Remedies could address the supply-side, e.g. by opening up monopolies or ecosystems or prevent markets from tipping. They could address the demand side problems, e.g. by targeting consumer behavioural biases and decision-making issues mentioned above. This could include information disclosure and presentational requirements to enable more self-determined decision-making and limit the exploitation of behavioural biases, facilitating consumer switching and protecting of consumers against unfair commercial practices. The effectiveness of consumer-facing remedies should be empirically verified.

Given the dynamic character, especially of digital markets, it is necessary to regularly monitor the effectiveness of the imposed remedies. This allows the remedies to be refined if proven ineffective or terminated if they no longer necessary.

Potential remedies could include:

- Data separation within ecosystems or conglomerate companies, including restrictions on usage/integration of consumer data obtained from different branches/services of a conglomerate company. For example where data has been collected through the leveraging of market power.
- Data portability, giving consumers control over data sharing and mobility (e.g. migrating data to another service).
- Unbundling/untying of services and terms of conditions, including in cases where consumers, in order to get access to a specific service, have to use/install a different service or accept terms and conditions allowing the firm to collect and analyse more consumer data than is necessary for the functioning of the service.
- Third parties' access to data where this is a barrier to entry (under strict adherence to the GDPR).
- Third parties' access to other inputs/services (under strict adherence to the GDPR).
- Prohibition/restrictions of self-preferencing of own services/products (e.g. in advertisement and specialised search).

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 to question 8 above.

Large gatekeeper platforms can take the form of conglomerate companies whose business activities fall under the competence of different regulatory and supervisory authorities at the Member State and EU levels. But nonetheless, some recently emerged digital services, posing significant challenges/risks for consumer welfare and competition alike, are not explicitly regulated or supervised by any specific competent authority. That holds for example for the “multi-purpose technology” of smart digital assistants. Another important factor for the enforcement of the Ex Ante Regulation is that many of the large players concerned are typically active in different Member States. This fact, however, does not automatically require the creation of a new competent authority. Instead, vzbv proposes to evaluate the idea of establishing a new Taskforce led by DG COMP to enforce the Ex Ante Regulation and the envisaged New Competition Tool (NCT).

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*

See answer to question 8 above.

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*

See answer to question 8 above.

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*

Yes, See answer to question 8 above.

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*

Also compare the answer to question 4 above.

Effective measures can include:

- Obligations to facilitate the exercise of the data portability rights under the GDPR. See: [http://www.beuc.eu/publications/beuc-x-2020-046\\_a\\_european\\_strategy\\_for\\_data\\_-\\_beucs\\_response\\_to\\_public\\_consultation.pdf](http://www.beuc.eu/publications/beuc-x-2020-046_a_european_strategy_for_data_-_beucs_response_to_public_consultation.pdf)
- Access to data where this is a barrier to entry.
- Giving consumers control over data sharing and mobility. Including obligation to support full data portability by consumers, including automated transfer of data to competitors upon consumers' request.
- Prohibition of practices of tying and bundling with respect to data.
- Data separation within a Firm: Restrictions on using/integrating consumer data obtained from different branches of a conglomerate firm or through different services.

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

*3000 character(s) maximum*

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

- Institutional cooperation with other authorities addressing related sectors – e. g. competition authorities, data protection authorities, financial services authorities, consumer protection authorities, cyber security, etc.
- Pan-EU scope
- Swift and effective cross-border cooperation and assistance across Member States
- Capacity building within Member States
-

High level of technical capabilities including data processing, auditing capacities

- Cooperation with extra-EU jurisdictions
- Other

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

*3000 character(s) maximum*

See answer to question 8 above.

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

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

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

*3000 character(s) maximum*

See answer to question 8 above.

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 checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>                               |
| 4. There is a need for a New Competition Tool allowing to address structural risks and lack of competition in (digital) markets on a case-by-case basis.   | <input type="radio"/> | <input type="radio"/>            | <input type="radio"/>      | <input type="radio"/>            | <input 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*

The European Commission should design the Ex Ante Regulation and the New Competition Tool (NCT) in a complementary manner:

a) A mix of general prohibitions/restrictions of certain unfair trading practices and targeted obligations for large online platforms acting as gatekeepers under the proposed Ex Ante Regulation envisaged in the DSA to tackle general problems.

b) Specific tailor-made remedies for large gatekeeper platforms on a case-by-case basis under the NCT to tackle structural competition problems.

Both, the Ex Ante Regulation and the NCT must also be complementary to the

c) Existing enforcement of Articles 101 and 102 TFEU of anticompetitive conduct.

The European Commission should complement “traditional” competition policy enforcement under Articles 101 and 102 TFEU with the NCT tackling case-specific structural problems (outside of the realm of Articles 101 and 102 TFEU) and an Ex Ante Regulation with general prohibitions/restrictions of certain practices and targeted obligations for large gatekeepers. This triple approach would create a legal and enforcement framework capable of addressing the blind spots of the current enforcement of competition law and set the conditions for consumer welfare to thrive in the digital economy and other markets.

vzbv emphasises that there should be no friction between the ex-ante rules and the NCT and that they should complement each other’s role in ensuring that markets are open, competitive and fair. Also, law makers must clearly distinguish between the enforcement of Articles 101 and 102 TFEU and the enforcement of the NCT.

27 Are there other points you would like to raise?

*3000 character(s) maximum*

Please see the attached submission for other points.

#### 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*

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

*3000 character(s) maximum*

vzbv recommendations are the following:

- Regulation should cover all categories of advertising, not just political ads.
- At the very least, consumers should have the same level of information than advertisers have when willing to place an ad. These should include the type of targeting criteria applied, who the source behind the ad is, etc.
- Once the Omnibus Directive becomes applicable, not disclosing paid advertisements or paid placement in ranking of search results in a clear, concise and intelligible manner will be considered as an unfair commercial practice. This transparency requirement applies to both direct or indirect payments by traders. To complement this, the Digital Services Act must impose an obligation on digital service providers to disclose who is paying for the ad and, if applicable, on behalf of whom they are placing it.

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

*3000 character(s) maximum*

See our previous response. We would like to highlight that information or transparency is not a panacea. The European Commission should focus on the business model, good design patterns, addressing competition concerns related to the ad market concentration in the hands of Google and Facebook and robust enforcement.

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

*3000 character(s) maximum*

Auditing by relevant competent authorities and third parties independent from the company such as consumer organisations.

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*

If properly enforced, it can contribute to achieve greater competition, more opportunities for smaller business, reduce the gatekeeping function of some platforms, contribute to more diverse views and reduce the number of illegal activities online.

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

*3000 character(s) maximum*

## **Smart contracts**

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

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



2 Please explain the difficulties you perceive.

*3000 character(s) maximum*

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

- Mutual recognition of the validity of smart contracts in the EU as concluded in accordance with the national law
- Minimum standards for the validity of “smart contracts” in the EU
- Measures to ensure that legal obligations and rights flowing from a smart contract and the functioning of the smart contract are clear and unambiguous, in particular for consumers

- Allowing interruption of smart contracts
- Clarity on liability for damage caused in the operation of a smart contract
- Further clarity for payment and currency-related smart contracts.

4 Please explain.

*3000 character(s) maximum*

5 Are there other points you would like to raise?

*3000 character(s) maximum*

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

---

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

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

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

1 What type of service do you offer through platforms?

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

2 Please explain.



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

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

- Yes
- No

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

- Yes
- No

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

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

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

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

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

*3000 character(s) maximum*

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

*3000 character(s) maximum*

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

*3000 character(s) maximum*

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

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

- Yes
- No

15 Please explain.

---

*The following questions are targeting online platforms.*

### **Role of platforms**

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

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

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

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

- Yes
-

No

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

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

### Rights and obligations

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

*3000 character(s) maximum*

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

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

25 Please explain.

*3000 character(s) maximum*

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

*3000 character(s) maximum*

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

*3000 character(s) maximum*

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

-

Yes

No

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

*3000 character(s) maximum*

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

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

*3000 character(s) maximum*

---

*The following questions are open to all respondents*

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

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

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

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

33 Please explain the issues that you encounter or perceive.

*3000 character(s) maximum*

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

- Yes
- No
- I don't know

35 Please explain and provide examples.

*3000 character(s) maximum*

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

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

*3000 character(s) maximum*

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

|                           |   |
|---------------------------|---|
| through online platforms? | <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> |
|                           |   |

in the offline/traditional economy?



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

3000 character(s) maximum

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

3000 character(s) maximum

40 Are there other points you would like to raise?

3000 character(s) maximum

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

---

The EU's Single Market offers a rich potential for digital services to scale up, including for innovative European companies. Today there is a certain degree of legal fragmentation in the Single Market . One of the main objectives for the Digital Services Act will be to improve opportunities for innovation and '[deepen the Single Market for Digital Services](#)'.

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

### Main issues

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

|  |  |
|--|--|
| Overall  |  |
| Those offered from outside of your Member State of establishment |  |

*The following questions are targeted at digital service providers*

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

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

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

|   | 1 (not at all burdensome) | 2                     | 3 (neutral)           | 4                     | 5 (very burdensome)   | I don't know / No answer |
|---|---------------------------|-----------------------|-----------------------|-----------------------|-----------------------|--------------------------|
| Different processes and obligations imposed by Member States for notifying, detecting and removing illegal content/goods/services | <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*

There is room for improvement. For example, some EU Member States or cities want to require companies like Airbnb to hold an estate agent's professional license so as to have more regulatory control over this type of platforms. However, in case C-390/18, the CJEU ruled Airbnb is an information society service under Art. 2, a) of the e-Commerce Directive. In this case, since France failed to notify the Commission about its law, the Court ruled France cannot impose such an obligation on Airbnb, as this would breach Article 3.4 b) of the e-Commerce Directive.

This case showed that the current e-Commerce Directive can create difficulties for Member States to adopt laws and policies to protect consumers. It is important however to note that the ruling should not be interpreted as meaning that governments cannot impose such measures on companies like Airbnb. The CJEU was clear that the notification obligation in the e-Commerce Directive "is not intended to prevent a Member State from adopting measures falling within its own field of competence and which could affect the freedom to provide services, but to prevent a Member State from impinging on the competence, as a matter of principle, of the Member State where the provider of the information society service concerned is established" (para. 95).

vzby's recommendations:

- Member States should keep being able to adopt laws protecting consumer interests. Public interest needs and market failures may vary from country to country so it is important to maintain derogations to the internal market clause of the e-Commerce Directive (Article 3 and the Annex).

- The consumer contracts derogation to the country of origin principle must be preserved (cf. Article 3 and the Annex of the current e-Commerce Directive), in line with the principles laid down in the Rome I Regulation. The country of origin principle covers the Directive's information obligations but does not apply to

contractual obligations concerning consumer contracts. For the latter, the consumer's home country law prevails if goods, services or digital content are targeted to that country and the consumer protection level is higher. This would be in line with Article 6 Rome I Regulation where, for consumer contracts, the applicable law is that of the country where the consumer has his/her habitual residence. This cannot be excluded by choice-of-law contract clauses, as following the Court of Justice of the European Union (CJEU)'s joined cases C-240/98 to C-244/98, contract terms which seek to supersede this are to be deemed as unfair under the EU Unfair Contract Terms Directive.

Any push to expand the scope of the Internal Market Clause to e.g. consumer protection/contracts would be an explosive paradigm change of EU consumer law. For Member States with stronger consumer protection laws, this would be very detrimental. Not only would their consumers lose the increased level of protection with regard to digital services from other Member States. But with an Internal Market Clause applicable to consumer protection/contracts there would be a strong incentive for consumer-targeting businesses to locate to the Member State with the least consumer protection, affording this Member State an economic advantage. The result would be a competition for the lowest possible consumer protection standard between Member States. On top of this, consumers would have to be proficient in the laws of all Member States to correctly assess their rights under EU consumer law, as opposed to just the laws of their home state. This would put consumer rights at a significant danger and lead to a sharp decline in consumer protection throughout the EU.

While consumer law has been more harmonised since 2000, EU law still leaves margin of manoeuvre to Member States to act so countries can address national, regional and local issues.

## 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 checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>    |
| Cooperation mechanism within Member States across different competent authorities responsible for the systematic supervision of online platforms and sectorial issues (e.g. consumer protection, market surveillance, data protection, media regulators, anti-discrimination agencies, equality bodies, law enforcement authorities etc.) | <input type="radio"/>    | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/>    |

|   |                       |                       |                       |                                  |                                  |                       |
|---|-----------------------|-----------------------|-----------------------|----------------------------------|----------------------------------|-----------------------|
| Cooperation mechanism with swift procedures and assistance across national competent authorities across Member States         | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/> |
| Coordination and technical assistance at EU level   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/> |
| An EU-level authority   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" 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 type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/> |
| Other: please specify in the text box below   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/> |

### 3 Please explain

*5000 character(s) maximum*

vzbv recognises that national authorities are crucial in enforcing Member States' consumer laws. However, digital services such as online platforms generally benefit from network effects and aim to reach as many potential customers at once. In pursuit of this goal, online platforms typically provide their services to EU consumers across Member States, not just directed at a single Member State.

Therefore the most impactful infringements of consumer protection laws are the ones that violate the basics of harmonised EU consumer law. vzbv believes that an independent, specialized supervision with appropriate sanctions should be introduced to ensure compliance with transparency and information obligations. This is especially true when transaction platforms enable suppliers from non-EU countries to conclude contracts directly with EU consumers.

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

*3000 character(s) maximum*

Like digital service providers, authorities should also make their work publicly available, sometimes at a later stage, as early disclosure could jeopardise the effectiveness of investigations. This information should include the number of actions taken on the basis of alerts by consumer organisations. This should complement an obligation on authorities to closely cooperate with civil society, not only with industry, as rightly pointed out by the Commission in question 2.

### 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*

vzbv supports that in the Communication on disinformation in times of COVID-19, the Commission and the EEAS said that, in the long term, it will look at providing a common toolbox for digital markets with specific tools to conduct online investigations and screen rogue practices. The Commission also committed to “consider open sourcing some of the tools it has developed to detect misleading narratives”. This idea can

be further developed by making data available to consumer organisations to help them in their watchdog functions/ making tools accessible to market watchdogs.

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*

vzbv believes that the considerations above hold even more true to digital services established outside the EU. There should also be no additional requirement such as "a significant number of users in the EU". Violations of consumer law in the EU must be able to be addressed by capable authorities and consumer organisations regardless of the number of incidents. That is why the answer should be "Yes."

The infringement of EU consumer law from non-EU-companies, which can be observed throughout many online platforms today, damages not only EU consumers. EU businesses are burdened with competition that gains commercial advantages by not playing by the same rules. The proposed EU-level authority would be an important step in enforcing EU consumer law to the benefit of everyone.

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*

In other laws, this issue is often addressed by first having a broad territorial scope of application of the law and then to ensure there is a responsible person/contact point in the EU that can be addressed by authorities /consumers/third parties. Finally, authorities must be provided with the necessary human, technical and financial resources to act.

For transaction platforms, the same tools would be needed as pointed out above (question 5). Compliance with EU laws and cooperation with EU authorities should be required from any service or goods provider aiming to conduct business in the common market.

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*

An option can be to have a network of national central authorities to coordinate amongst each other like the CPC network.

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*

In the area of consumer protection, cross-border and widespread in the EU infringements can be addressed by the Consumer Protection Cooperation (CPC) network of national authorities. The authorities cooperate in investigations and taking enforcement measures or obtaining commitments from the traders to change practices. Consumer associations regularly inform the CPC authorities about the cross-border infringements and ask them to take action. However, there is usually no feedback on what the authorities are going to do, and this issue prevents a more efficient cooperation.


In the area of product safety, BEUC regularly informs the European Commission about results from consumer research and testing and asks the Commission to share those results with the national market surveillance authorities in charge. This concerns information about non-compliant and dangerous consumer products such as toys, cosmetics and electric appliances. Cooperation at national level varies among EU Member States from transparent and inclusive consultations of consumer groups to insufficient levels of cooperation. It is not easy for consumer organisations to obtain transparent information from national market surveillance authorities about the follow up to the actions.





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

*3000 character(s) maximum*

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

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

|   |   |
|---|---|
| Coordinating the handling of cross-border cases, including jurisdiction matters |  |
|   |   |

|  |   |
|--|---|
| Agreeing on guidance for consistent implementation of rules under the AVMSD                      |   |
| Ensuring consistency in cross-border application of the rules on the promotion of European works |  |
| Facilitating coordination in the area of disinformation  |  |
| Other areas of cooperation   |  |

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

*3000 character(s) maximum*

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

*3000 character(s) maximum*

## Final remarks

---

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

### 1 Upload file

The maximum file size is 1 MB

Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

**0e0a45c9-4dab-45be-8236-9299edea5cc1/20-09-03\_vzbv\_Positionspapier\_DSA\_Konsultation.pdf**  
**00398817-84d5-49e3-9a8f-03f1515b5e40/20-09-07\_vzbv\_Statement\_DSA\_Gatekeepers\_New\_Competition\_Tool.pdf**

### 2 Other final comments

*3000 character(s) maximum*

## Useful links

## **Background Documents**

[\(BG\) Речник на термините](#)

[\(CS\) Glosř](#)

[\(DA\) Ordliste](#)

[\(DE\) Glossar](#)

[\(EL\) ά](#)

[\(EN\) Glossary](#)

[\(ES\) Glosario](#)

[\(ET\) Snastik](#)

[\(FI\) Sanasto](#)

[\(FR\) Glossaire](#)

[\(HR\) Pojmovnik](#)

[\(HU\) Glosszrium](#)

[\(IT\) Glossario](#)

[\(LT\) Žodynėlis](#)

[\(LV\) Glosārijs](#)

[\(MT\) Glossarju](#)

[\(NL\) Verklarende woordenlijst](#)

[\(PL\) Słowniczek](#)

[\(PT\) Glossrio](#)

[\(RO\) Glosar](#)

[\(SK\) Slovnk](#)

[\(SL\) Glosar](#)

[\(SV\) Ordlista](#)

## **Contact**

CNECT-consultation-DSA@ec.europa.eu



