

Digital Services Act package: open public consultation

Fields marked with * are mandatory.

Introduction

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

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

T h i s

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

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

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

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

Digital services and other terms used in the questionnaire

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

* 2 I am giving my contribution as

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

* 3 First name

Gabrielle

* 4 Surname

Guillemin

* 5 Email (this won't be published)

gabrielle@article19.org

* 7 Organisation name

255 character(s) maximum

ARTICLE 19

* 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.

594787238502-76

* 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

3 Please specify.

3000 character(s) maximum

N/A

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

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



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

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



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

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



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

- Yes
- No

8 Please explain

3000 character(s) maximum

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

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

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

5000 character(s) maximum

Illegal content

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

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

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

3000 character(s) maximum

ARTICLE 19 has generally not responded to questions in section A as we do not engage in flagging of potentially illegal content. However, we are aware that some individuals, particularly women journalists, are having difficulties reporting gender based harassment online.

More generally, we believe that Internet users cannot answer this question with any degree of accuracy and should not be asked to do so. Whether or not content is 'illegal' can only be determined by a court or an independent adjudicatory body. In addition, with the exception of certain specific categories of child sexual abuse material, the lawfulness of most of the other categories of content highlighted above is highly dependent on context and other factors (e.g. in case of incitement, inter alia position of the speaker and his /her influence over the audience). To give an example, some content online may be defamatory but it could be justified by reference to fair comment or some other defence so that it would not be unlawful.

ARTICLE 19 is concerned that the outbreak of COVID-19 has led social media companies to rely increasingly on automated filters. Since filters remain intrinsically unable to take context properly into account, it will inevitably lead to an increase in wrongful removals of content. This is especially concerning since companies such as Facebook have suspended their appeals mechanisms in that period. For more details, see here: <https://www.article19.org/resources/coronavirus-tech-companies-should-use-manila-principles-to-manage-misinformation/>

In any event, ARTICLE 19 believes that the European Commission cannot seriously address the issue of content regulation without first acknowledging and tackling head on the business model of online platforms as a matter of priority. We note that a number of human rights organisations, including ARTICLE 19, have called for a radical overhaul of this business model, that is based on the collection of vast amounts of data about their users and its monetisation through online (targeted) advertising, because it significantly impacts human rights.

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

There is insufficient information at present to understand the real impact of the measures put in place by the social media companies with significant market power during the period of COVID-19 pandemic. For instance, there is currently no COVID-19-specific transparency report being published by the social media platforms with significant market power. ARTICLE 19 has outlined our concerns in relation to Facebook transparency reporting in more detail here: <https://www.article19.org/resources/facebook-improvements-in-transparency-reporting-more-urgent-amid-coronavirus-pandemic/>

Nonetheless, we note that, since the COVID-19 outbreak, social media companies such as Twitter or Facebook have engaged more regularly with international organisations such as the World Health Organisation, and civil society organisations such as ours. This can contribute to the dissemination of more reliable information and the development of more human rights compliant policies respectively.

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

N/A

21 Do you consider these measures appropriate?

- Yes
- No
- I don't know

22 Please explain.

3000 character(s) maximum

B. Transparency

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

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

3 Please explain.

3000 character(s) maximum

ARTICLE 19 regularly receives requests from Internet users, including journalists, artists and activists, whose content has been removed by Facebook or Twitter. More often than not, we are told that those users discovered one day that their account had disappeared with no information being given. Even when some information is received, it is generic with no explanation or reasons being given as to why the content was removed.

A telling example concerns an Italian journalist, Mariano Giustino, who was commenting on Turkish politics. Mr Giustino posted the following comment: “Turkey: last night, thanks to the law on penal execution, organised criminal and member of the Grey Wolves, Alaattin Çakıcı, was released from prison. This new law has allowed 90,000 prisoners to have their sentences reduced, but not journalists, politicians from the opposition and human rights activists @RadioRadicale”.

Immediately after posting this message, Giustino’s Facebook account disappeared. After he requested an explanation, Mariano received the following message:

“We have received your information. If we notice that your account does not respect our Community Standards it will stay disabled. We always take care of security on Facebook, even when you aren’t able to use your account”.

Giustino repeatedly tried to contact Facebook to find out why his account was closed. It took over forty days for it be reinstated; he still doesn’t know why it was closed in the first place or whether it will happen again. (For full story, see here: <https://www.article19.org/resources/mariano-giustino-journalist-censored-by-facebook/>).

ARTICLE 19 staff have also had their Facebook account removed after trying to upload a video as part of our Missing Voices campaign, which ironically seeks to raise awareness about censorship on social media platforms. Facebook also blocked the uploading of ARTICLE 19 campaign videos raising awareness about artistic censorship. The video featured the work of Borghildur Indriðadóttir, an Icelandic visual artist whose work was censored by Facebook in 2018 because it breached Facebook’s nudity and nipple ban.

ARTICLE 19’s Missing Voices campaign calls for more transparency and the improvement of internal complaint mechanisms when social media platforms remove content and close down users’ accounts under their policies and community guidelines. For more stories of wrongful removals of content, see here: <https://www.article19.org/campaigns/missingvoices/>

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

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

5 When content is recommended to you - such as products to purchase on a platform, or videos to watch, articles to read, users to follow - are you able to obtain

enough information on why such content has been recommended to you? Please explain.

3000 character(s) maximum

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

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

3000 character(s) maximum

ARTICLE 19 notes at the outset that the recently reviewed AVMSD expressly mandates online video-sharing platforms services to put in place ‘appropriate’ measures, such as age verification and parental control systems, to protect children from material that may impact their physical, mental or moral development. ARTICLE 19 understands the concerns of child protection organisations around the availability of ‘harmful’ material online and their potentially negative impact on the development of children. Nonetheless, we are worried that proposals for greater regulation in this area could entrust a regulator with powers to decide what amounts to ‘harmful’ content online in the absence of primary legislation to that effect. For instance, it is highly unclear what ‘self harm’ means or what form it might take, e.g. whether it includes websites about anorexia, alcoholism, drug taking or dangerous sex. Moreover, while the idea of removing ‘self-harming’ websites may sound attractive, in practice, educational websites about this issue may end up being caught in filters that are currently unable to capture such nuance (see, for example a joint submission of ARTICLE 19 and Prostasia foundation, <https://prostasia.org/wp-content/uploads/2019/12/Prostasia-case-and-Paypal-submission-December-2019.pdf>). Equally, youth who visit self-harm websites may be joining online groups to share experiences and connect with others. Although some of these conversations may be unhealthy, others may not be. Shutting down such websites could therefore have a detrimental impact on such youth looking out for a sense of community and belonging.

ARTICLE 19 is also concerned about mandatory technical solutions, such as proactive filtering or age-verification systems that could have a disproportionate impact on the privacy and free speech rights of both children and adult Internet users. We are equally concerned about any proposals that could both undermine encryption and/or online anonymity. In our view, these are cornerstones of the protection of freedom of expression, privacy and information security online and should be strongly protected.

Instead, we believe that social media companies should continue to adopt measures such as content rating and parental control systems on a voluntary basis. They should also be more transparent about their content moderation practices and provide complaints mechanisms for wrongful removal of content or for when they refuse to take content down. In addition , they should contribute to media literacy efforts for both parents and children. (For details of ARTICLE 19’s views on preventing ‘online harms’ for children, see Malcolm and Guillemain, Internet companies alone can’t prevent online harms, April 2020: <https://www.article19.org/resources/internet-companies-alone-cant-prevent-online-harms/>)

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

3 Please explain.

3000 character(s) maximum

ARTICLE 19 notes that reference to 'online platforms' in the table seems to be written with social media platforms with significant market power- such as Facebook or Twitter - in mind whereas there are many more platforms operating in the EU. The last statement about online platforms "guaranteeing" a "sufficient" degree of democratic integrity, pluralism, tolerance, justice, solidarity and gender equality seems to imply that they all have or should have duties similar to that of public authorities. It is unclear that this should be the case, at least for all platforms regardless of their size or in relation to all areas listed. In particular, we note that by and large the terms "democratic integrity", "tolerance", "justice" and "solidarity" are extremely broad and without definition for the purposes of this consultation. Even reference to non-discrimination and gender equality is unclear, i.e. it fails to distinguish between access to the service itself, which platforms would presumably be required to comply with as a matter of law, and content moderation practices related to 'hate speech' posted by other users. In any event, it is hard to know whether online platforms can be trusted as we know too little about their practices.

ARTICLE 19 believes that 'online platforms' should respect international human rights standards as set out in the UN Guiding Principles on Business and Human Rights (for more details, please see ARTICLE 19's policy "Sidestepping Rights: Regulating Speech by Contract" (2018): <https://www.article19.org/resources/side-stepping-rights-regulating-speech-by-contract/>)

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

As noted above, ARTICLE 19 does not engage in flagging potentially 'harmful' content, so we are not in a position to answer this question. We note however that it is very difficult to answer this question accurately as the amount of 'harmful' content on a platform is likely to change everytime the platform changes its definition of content it considers unacceptable under its community standards. In general, platforms have tended to expand the definition of content considered 'harmful' under those standards, especially during the COVID-19 outbreak. In practice, this means that more content is considered 'harmful' and gets removed.

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

3000 character(s) maximum

There have been some positive initiatives to tackle misinformation related to the COVID-19 outbreak. In January 2020, the WHO launched the 'WHO Information Network for Epidemics'(EPI-WIN), its program to combat misinformation by providing "timely accurate information from trusted sources." The WHO is also partnering with tech companies including Facebook, Google, Tencent, Baidu, Twitter, TikTok, Weibo, Pinterest, as well as online 'influencers', to promote accurate information about COVID-19. Major social media platforms have taken steps to promote authoritative content about the virus in news feeds and reduce the visibility of misinformation (e.g. Facebook has been placing 'education pop-ups' featuring information from the WHO and national health authorities at the top of result pages for searches relating to the coronavirus. Likewise, Twitter has been promoting credible information at the top of search results).

D. Experiences and data on erroneous removals

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

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

5000 character(s) maximum

There is still very limited information available about the scale of wrongful removals of content, particularly as it relates to particular regions or countries. The only information available stems from broad figures about successful appeals against takedowns. For instance, in its last Transparency report (Jan-March 2020), Facebook reported the following:

- Content reinstated on appeal has decreased for nudity -related content: whereas nearly 4 million pieces of content had been appealed in April-June 2019, it was down to about 2.3 million in January-March 2020. The number of pieces of content restored has also decreased from just over one million in April-June 2019 to just over 600,000 in January-March 2020.

- The number of appeals on hate speech grounds remains stable, hovering around 1.3 million between January-March 2019 and the same period in 2020. Since a peak of around 170,000 pieces of content restored in July-September 2019, the number of reinstated content has steadily decreased to just over 60,000.

- Appeals against decisions on organised hate have increased but not led to a significant amount of reinstated content. Appeals against actioned content on grounds of organised hate have increased since October-December 2019 reaching just over 230,000 in January-March 2020. The amount of restored content is low, at about 50,000 pieces of content. Some content is restored automatically, primarily terrorist-related content with nearly 300,000 pieces of content restored without appeal.

Our Missing Voices Campaign has collected stories of wrongful removals of content on the basis of companies' community standards. There are regular examples of journalists, artists, human rights defenders and marginalised groups experiencing the wrongful removal of content. This undoubtedly has an impact on their fundamental rights and ability to do their job effectively, including by holding governments and others to account. More information about the Missing Voices Campaign is available from here: <https://www.article19.org/campaigns/missingvoices/>

The following questions are targeted at organisations.

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

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

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

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

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


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

3000 character(s) maximum

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

- Yes
- No
- I don't know

13 How valuable is this information for you?

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

14 Do you use or 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

ARTICLE 19 is concerned about this question. It seems to suggest that the Commission is considering the adoption of measures that would effectively enable law enforcement to gain access to data about users that would reveal what content they are viewing. This could be then deemed by a platform or law enforcement as the 'wrong' kind of content, regardless of intent or purpose of the user who posed or shared it. In our view, this would amount to unlawful surveillance in breach of international standards on freedom of expression and privacy.

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

ARTICLE 19 is concerned that this question seems to suggest that the Commission is looking to dictate what content platforms should ban under their terms of service or Community Guidelines. If so, this would be tantamount to legislating by the backdoor and ultimately delegating censorship powers to private companies. If policy-makers are sufficiently concerned about certain types of content, they should do so through the democratic process, i.e. adopt laws banning such content in line with the requirements of the EU Charter of Fundamental Rights and European and international human rights standards, particularly the legality principle.

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

ARTICLE 19 welcomes this question. We believe that quality standards should be both transparent and subject to human rights impact assessments, including their error rate and whether they render large quantities of information inaccessible. Information about error rates (i.e. both false positives and false negatives) could also be parsed from successful appeals against wrongful takedowns on the basis of automated detection and removal tools. Moreover, we believe that at a minimum the use of automated filters by private companies should include a 'human in the loop' for reviewing content moderation decisions. Please see also our response to Q6 of section II on the review of the liability regime for Internet intermediaries.

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

ARTICLE 19 believes that far more information about automated tools should be made available. The enormous information asymmetry around those tools is creating numerous challenges. From an economic perspective, it alters power dynamics in the market, raising barriers to entry and locking in consumers. From a societal perspective, it violates the autonomy and informational self-determination of consumers, who are not aware of how those mechanisms work and how that impacts what they see, access and share on the

platforms. Mandating meaningful transparency is a fundamental step to address these challenges.

In particular, we believe that platforms should publish information about the way in which their algorithms operate to detect illegal or allegedly 'harmful' content under their community standards. This should include information about rates of false negatives/false positives and indicators, if any, to assess content that is likely to become viral, e.g. by reference to exposure to a wider audience. More generally, online platforms should explain to the public how their algorithms are used to present, rank, promote or demote content. Content that is promoted should be clearly marked as such, whether the content is promoted by the company or by a third-party for remuneration.

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 type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Have content moderation teams, appropriately trained and resourced	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Systematically respond to requests from law enforcement authorities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" type="radio"/>
In particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Request professional users to identify themselves clearly ('know your customer' policy)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide technical means allowing professional users to comply with their obligations (e.g. enable them to publish on the platform the pre-contractual information consumers need to receive in accordance with applicable consumer law)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Inform consumers when they become aware of product recalls or sales of illegal goods	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Cooperate with other online platforms for exchanging best practices, sharing information or tools to tackle illegal activities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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

"Cooperation" with national authorities is a very vague term that should not be used to require companies, whether big or small, to pass on to law enforcement agencies every allegation of illegality that they receive themselves. This would not be efficient since this would inevitably include allegations about minor offences.

An obligation to "cooperate" also suggests that companies may be required to respond to mere "requests" from law enforcement agencies as opposed to court orders. In our view, this would be inappropriate. Instead, illegal criminal content should be removed following an order of a court or an independent adjudicatory body. If the situation is urgent, for example because someone's life is at risk, law enforcement agencies should be given statutory powers to order the immediate removal of content but any such order should be confirmed by a court within a limited period of time, e.g 48 hours.

If "cooperation" implies access to data, we believe that proper procedures should be put in place. In particular, law enforcement authorities should not be able to access user data upon mere request but should obtain a court order.

Similarly, we don't believe that companies should be required to respond "systematically" to "requests" from law enforcement authorities. Currently, if law enforcement authorities make a "request" to remove content under social media platforms' community standards, those companies are not required to either respond or takedown the content. By making it an obligation to "respond", it is highly likely that "requests" would be understood as akin to orders to remove. It would be very similar to a notice and action system for law enforcement. While failure to respond occasionally would not necessarily be penalised, it would still effectively allow law enforcement authorities to bypass proper procedures in order to obtain the removal of content. In our view, online platforms should only be required to remove content when ordered to do so by a court.

Finally, we note that online platforms should generally be required to put in place an effective appeals mechanism against wrongful content takedowns. Law enforcement authorities should not be allowed to send requests to online platforms outside of the appropriate legal framework involving courts or other independent judicial authorities such as using the notice and action (N&A) mechanism to flag potentially illegal content. Instead, when law enforcement agencies find potentially illegal online content or behaviour online, they should go through proper due process channels. That's because when public authorities restrict fundamental rights by using their formal powers (e.g. to demand the removal of online speech or prosecute suspects), their powers are and should be limited by due process safeguards prescribed by law. Allowing law

enforcement officers to use the N&A mechanism would systematically bypass those safeguards. What is more, research has shown that content removal requests by police are four times more likely to be successful than other users' requests—indicating that platform operators either reduce the thoroughness of their own verification when removal requests come from police officers or just blindly trust that law enforcement officers make no mistakes. This kind of anticipatory obedience by platform operators increases the risk of abuse and politically motivated censorship. When issuing an order to remove or block access to an illegal piece of content, law enforcement should therefore require prior judicial authorisation by a court or an independent judge.

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

A notice should include the reason why the activity is considered illegal, including where possible the legal basis for the alleged unlawful conduct. In cases such as copyright or defamation, consideration should be given to asking notifying parties why they believe defences do not apply (e.g. fair comment, parody etc.).

The name and contact details of the notice provider should be required and passed on to the content provider in cases involving intellectual property or defamation claims. In the case of intellectual property, this would be partly to prevent the stem of abusive notices and in the case of defamation, because the identity and reputation of the person concerned is at the heart of the complaint (i.e. how they are held in the esteem of the wider public). More generally, it should be required for the purposes of processing the complaint but would not need to be included in all cases, where revealing the identity of the notice provider is neither necessary for the purposes of further legal action or where it could put their health and safety at risk (e.g. cases of domestic violence or other domestic abuse).

Other requirements should include additional evidence depending on the type of content at issue, e.g. evidence of offline violence that occurred as a result of online behaviour.

Finally, notice providers should be required to sign a declaration of good faith in relation to the content being reported as illegal. Abusive notices should be penalised, e.g. through a civil fine, and compensation paid to the injured party where appropriate.

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

ARTICLE 19 believes that the DSA should not require online platforms to prevent the reappearance of 'illegal' content. It would almost inevitably involve the use of automated filters and in practice, it would be tantamount to mandating their use. In our view, this would be both ineffective and disproportionate since filters are currently incapable of distinguishing the legality of content depending on its context. In practice, it is highly likely that large amounts of legitimate content would get caught.

In our view, 'specific' monitoring may only be justified when it is used to detect and remove videos or other images of child sexual abuse in circumstances where the material is uncontroversially unlawful regardless of context (i.e. depiction of sexual activity between a child and an adult, such as penetration). This is also because of the gravity of the content at issue.

We further note that in the *Glawischnig-Piesczek v Facebook* case, the CJEU found that a Member State's court could order 'specific monitoring' of content that is identical or equivalent to content found unlawful. As far as 'equivalent' content is concerned, the Court seemed to suggest that an 'equivalent content' order should include a list of words, expressions and other content deemed 'equivalent' by the court to the expression found to be unlawful and that the hosting provider is required to block it by way of automated detection. See for instance this analysis by Bird & Bird: <https://www.twobirds.com/en/news/articles/2019/global/notice-and-stay-down-orders-and-impact-on-online-platforms>

ARTICLE 19 believes, however, that the practical impact of the CJEU's decision in *Glawischnig-Piesczek v Facebook* is to mandate general monitoring since it is unclear how filters can look for 'specific', 'identical', let alone 'equivalent' content without filtering all content. Moreover, we believe that the Court was mistaken in assuming that the same or 'identical' image or text is always unlawful regardless of its context. In any event, what amounts to 'equivalent' content should at the very least be determined in advance by a court.

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?

Social media companies use a number of different automated tools, including natural language processing (NLP) for text-based content and hash databases of image or video content, among others. Their shortcomings are well-known and include their inability to understand context and intent, both of which are vital to determinations about the legality of speech. Depending on the data being used to train them, they can also entrench human biases and amplify them, so that minority groups are at greater risk of being censored and further marginalised. It is also worth noting that most NLP works most effectively in English but less well in other languages, resulting in greater error rates. The shortcomings of NLP have become particularly apparent in the context of the COVID-19 crisis with social media companies with significant market power recognising that more errors may occur in the removal of content. (see ARTICLE 19, *Coronavirus: Manila Principles should be used to manage misinformation*, March 2020: <https://www.article19.org/resources/coronavirus-tech-companies-should-use-manila-principles-to-manage-misinformation/>)

For the shortcomings of NLP, we refer to CDT's in-depth analysis in their *Mixed Messages* report, available from here: <https://cdt.org/wp-content/uploads/2017/11/Mixed-Messages-Paper.pdf>

Notwithstanding the above, we recognise that automated tools provide an opportunity to reduce the psychological toll on content moderators who are tasked with watching or reviewing content for hours, often in poor working conditions. See for instance, Isaac Chotiner, *The Underworld of online content moderation*,

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

ARTICLE 19 believes that the EU should not adopt measures that would have the effect of restricting freedom of expression beyond the EU's borders where that content would be lawful.

We also urge caution against applying EU rules to digital services established outside of the EU in circumstances where this would lead other, less democratic, countries to do the same. We are concerned that this could lead to conflicts between the various rules applicable to platforms providing digital services globally and ultimately have negative consequences for freedom of expression worldwide. In other words, it could significantly undermine one of the Internet's greatest achievements, namely to make the right to freedom of expression truly borderless and instead erect EU borders.

We also believe that this could lead to EU consumers being deprived of greater choice of content, goods and services outside the EU. Depending on the scope of the DSA, it could mean for instance that the New York Times has to comply with a number of obligations under the DSA because it has more than a certain number of users in the EU and its news articles offer a comment section. Faced with burdensome obligations, it is not impossible to imagine that it would make the choice of discontinuing the offer of certain services to individuals established in the EU.

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

ARTICLE 19 believes that companies providing essential Internet infrastructure services, such as content delivery networks, should benefit from broader immunity from liability than providers that are engaged in content moderation at the application layer. They should only be required to remove content by order of a court. In practice, this means that infrastructure providers, such as Cloudflare, should not be penalised for hosting websites such as 8chan or DailyStormer, unless they have failed to comply with a valid court order requiring them to discontinue their services to such a website. Equally, they should not be required to host such a website if they do not wish to do so, except in circumstances where no other alternatives are available. In other words, infrastructure providers should not be mandated to carry content, save where the service they provide is deemed essential by a court for the promotion of pluralism and diversity and there is no other alternative for that content to be hosted. When infrastructure service providers decide to discontinue the provision of their services, they should at least clearly set out the reasons why they have done so. More

generally, they should respect international human rights standards in this area as explained in more detail by ARTICLE 19 in our policy “Getting connected: Freedom of expression, telcos and ISPs” (July 2017): <https://www.article19.org/wp-content/uploads/2017/06/Final-Getting-Connected-2.pdf>

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

At the outset, we note that national authorities do not have 'rights' under human rights law. The powers and responsibilities of national authorities should be clearly set out in the law and be necessary and proportionate to their mission, which should be consistent with the legitimate aims under the EU Charter of fundamental rights. In practice, this means, among other things, that the law granting powers to national authorities should include a clear reference to the protection of human rights as part of their mission. Moreover, for national authorities to be effective, they need to be adequately resourced and be equipped with appropriate knowledge, expertise and skills in order to be able to address the specific challenges posed by social media platforms and other internet actors. Finally, we note that in a shared regulatory space such as that of online platforms, it is vital for the various national authorities involved (e.g. competition, data protection, elections, equality bodies etc.) to cooperate and coordinate.

It is not the role of third-parties or civil society to "tackle" illegal activities. In our view, for instance, trusted flaggers should not be considered as an extension of law enforcement. Similarly, their assessment of the lawfulness of content should not be equated with that of a court decision or taken as having the same binding effect. Similarly, it is important to remember that trusted flaggers are not independent since they defend a particular viewpoint or interest. To the extent that trusted flaggers are being used, consideration should be given to employing a kitemark certification system on a self-regulatory basis to indicate that organisations engaging in flagging illegal content fulfil certain quality standards. Law enforcement authorities should not qualify as trusted flaggers and should use legal procedures to order the removal of content.

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

ARTICLE 19 believes that legal but harmful content should be out of scope of the DSA. To the extent that it is included, we believe that any obligations imposed on social media platforms should be limited to:

Transparency obligations, specifically:

1. Distribution of content: digital companies should provide essential information and explain to the public how their algorithms are used to present, rank, promote or demote content. Content that is promoted should be clearly marked as such, whether the content is promoted by the company or by a third-party for remuneration. Companies should also explain how they target users with (unsolicited) promoted content, whether at their own initiative or on behalf of third parties as a paid service. Equally, companies should clearly highlight content whose reliability is in doubt or content that has been fact-checked.

2. Companies' terms of service and community standards: companies should publish community standards/terms of service that are easy to understand and give "case-law" examples of how they are applied. They

should publish information about the methods and internal processes for the elaboration of community rules, which should continue to include consultations with a broad range of actors, including civil society.

3. Human and technological resources used to ensure compliance: companies should include detailed information about trusted flagger schemes, including who is on the roster of trusted flaggers, how they have been selected and any 'privileges' attached to that status. They should also publish information about the way in which their algorithms operate to detect illegal or allegedly 'harmful' content under their community standards. In particular, this should include information about rates of false negatives/false positives and indicators, if any, to assess content that is likely to become viral, e.g. by reference to exposure to a wider audience.

4. Decision-making: companies should notify their decisions to affected parties and give sufficiently detailed reasons for the actions they take against particular content or accounts. They should also provide clear information about any internal complaints mechanisms.

5. Transparency reports: companies should publish detailed information consistent with the Santa Clara Principles. It is particularly important not to limit statistical information to removal of content but also include data about the number of appeals processed and their outcome. Transparency reporting should also distinguish between content flagged by third-parties (including whether they are public bodies or private entities), trusted flaggers (whether public bodies or private entities) or algorithms. Further information should also be provided in relation to the different types of restrictions applied to content as part of content moderation processes, such as demonetisation or downgrading; for every restriction, the company should give information about the rules on the basis of which the decision was made and, where available, the outcome of any appeals.

More generally, we note that any transparency reporting requirements should aim to provide far more qualitative analysis of content moderation decisions. It is vital that the metric of success in addressing illegal content is not tied to content removal rates as it encourages over-removal. Equally, transparency reporting should not be limited to information submitted by companies but should include information submitted by relevant government agencies

6. Algorithms transparency audits: companies should give greater access to datasets for regulators and vetted independent researchers, whether academics, journalists or otherwise, in order for them to verify that the company's systems and algorithms are operating as the company says it does. In particular, auditors should be given access to data about: (i) companies' content moderation programmes; (ii) how companies order, rank, prioritise, recommend or otherwise personalise content; and (iii) how this applies to political advertising. Whilst regulators could be given access to sensitive and commercial data, vetted third-parties could be given access to anonymised datasets. These audits of platforms' operations should take place on a regular basis.

Internal due process obligations:

1. Clear notice and takedown rules in line with the Manila Principles on Intermediary Liability;

2. Internal redress mechanisms to deal with complaints about wrongful removal of content or the wrongful application of labels that would suggest that a news source is untrustworthy. Conversely, appeals mechanisms should also be able to address a company's refusal to remove content that is arguably in breach of the company's community standards.

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

ARTICLE 19 would urge against assuming that the removal or filtering of content deemed 'harmful' by a regulator is necessarily a proportionate response to 'potentially harmful' activities or content concerning minors. For instance, we note that websites about self-harm or other mental health issues, such as food disorders, can help young people talk about their experiences. It is therefore vital for the various parties involved to engage in continuing dialogues about the best approaches to address these issues. In our view, this would necessarily involve significant investment in education and media literacy programmes.

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 checked="" type="radio"/>	<input 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 checked="" type="radio"/>	<input type="radio"/>	<input 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 checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Adapted risk assessments and mitigation strategies undertaken by online platforms	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ensure effective access and visibility of a variety of authentic and professional journalistic sources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Auditing systems for platform actions and risk assessments	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input 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 checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other (please specify)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

13 Please specify

3000 character(s) maximum

ARTICLE 19 is concerned that regulatory oversight would almost inevitably involve the use of targets for removal of disinformation or fake accounts. This is suggested as a possible indicator in the May 2020 study for the assessment of the implementation of the Code of Practice on Disinformation (see page 94, available from here: <https://ec.europa.eu/digital-single-market/en/news/study-assessment-implementation-code-practice-disinformation>). It would also be consistent with the Commission's approach to monitoring of the implementation of the EU Code of Conduct on Countering Illegal Hate Speech (see e.g. latest round of monitoring here: https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf).

Given the lack of agreed definition of 'disinformation', this is a significant concern since it would ultimately encourage censorship of content which is not illegal per se and whose impact on democracies remains contested.

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

ARTICLE 19 is concerned by the lack of definition of what amounts to a 'crisis' or a 'systemic threat to society'. We are not reassured by the 'fast spread of illegal and harmful activities' being mentioned as an example. We are further concerned that no attempt has been made at defining what 'cooperation' might mean in this context. We would remind the Commission that any restriction on freedom of expression or the right to privacy must be clearly and narrowly defined by law, pursue a legitimate aim and be necessary and proportionate to that aim. The lack of definition of key terms is unlikely to meet the legality test. Moreover, the terms 'crisis' or 'systemic threat to society' do not correspond to the exhaustive list of legitimate aims

under Article 10 (2) ECHR. If EU Member States wish to derogate from their obligations under the European Convention on Human Rights in times of an emergency threatening the life of the nation, they must meet both substantive and procedural requirements as set out here:

https://echr.coe.int/Documents/FS_Derogation_ENG.pdf

We further urge caution against ad hoc protocols in 'crisis' situations since they usually involve fast removal of content in breach of international standards on human rights, especially freedom of expression, due process and the right to privacy. For instance, the New Zealand government set up an initiative, the 'Christchurch Call to eliminate terrorist and violent extremist content online', in the wake of a terrorist attack in Christchurch. This led to the development of an incident protocol to deal with the reproduction of the livestreaming of the attack. That protocol has now been established as part a new entity, the Global Internet Forum on Counter Terrorism. ARTICLE 19 is a member of the Advisory Network to the Christchurch Call. We have raised various concerns with the incident protocol, including the use of upload filters and the danger that legitimate content from broadcast media and others might get wrongfully removed.

More recently, we have joined several other human rights organisations in raising concerns about the lack of transparency in the way in which GIFCT operates, including in its engagement with law enforcement agencies, among others: <https://cdt.org/insights/human-rights-ngos-in-coalition-letter-to-gifct/>.

More generally, ARTICLE 19 is concerned about 'cooperation' being a by-word for sidestepping procedural safeguards for users' rights.

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

	1 (not at all necessary)	2	3 (neutral)	4	5 (essential)	I don't know / No answer
High standards of transparency on their terms of service and removal decisions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Diligence in assessing the content notified to them for removal or blocking	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input 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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

deployed for detecting, removing or demoting content or suspending users' accounts						
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 checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

16 Please explain.

3000 character(s) maximum

It is not clear to us what 'diligence in assessing content for removal or blocking' means. ARTICLE 19 has long highlighted concerns with unduly short removal timeframes as they do not allow for due process to take place *before* removal and do not allow for proper consideration of the complexity of the issues in highly context specific cases, e.g. 'hate speech'. As such, they are not conducive to the protection of freedom of expression.

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

5000 character(s) maximum

The Commission should consider mandating social media companies with significant market power to carry out human rights impact assessments throughout their operations, including their content moderation systems.

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

Please see our response to Q10.

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

Please see our response to Q10.

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

5000 character(s) maximum

ARTICLE 19 is concerned about a regulatory authority being able to dictate to social media companies what content they should be recommending, particularly in those countries where such authorities may not be independent or in countries where the rule of law is significantly weakened, such as Hungary or Poland.

In general, we support measures that promote greater media pluralism and media diversity whilst giving users greater choice over what they get to see. For this reason, we support an obligation imposed on large social media platforms to promote content diversity: Given the risks of overly personalised content on social media platforms, large social media companies should be required to take steps to ensure users are exposed to sufficiently diverse content and balanced coverage of issues of public interest on their service by default. This obligation should only be imposed in situations of market dominance and where it is necessary to support the online visibility of the broad diversity of viewpoints and opinions in society and with a view to enabling individuals to make informed decisions. In particular, as noted above, social media companies should provide sufficient information to explain how newsfeeds and the material they promote is selected. At the same time, individuals should be able to change content diversity default-settings easily in order to tailor their newsfeeds to their own interests and preferences. We also suggest that a multi-stakeholder forum such as the Social Media Councils (SMCs) can serve to elaborate the appropriate approach to content diversity on social media platforms.

Finally, ARTICLE 19 notes that in our view, companies should benefit from broad immunity from liability for the recommendations or suggestions made by their algorithms, even in circumstances where those algorithms recommend illegal content in response to content viewed by users. Whilst system developers and coders define the parameters within which 'algorithms' operate, they do not control or determine the outcome of these automated processes. Algorithms produce results from datasets in ways which are both complex and unpredictable. They are also both generally prone to making mistakes and unable to distinguish between lawful or unlawful content. Holding companies liable for every possible 'mistake' made by their systems would therefore be both unworkable and disproportionate. Insofar as liability deals with specific instances of illegality, it is also a poor instrument to address the systemic challenges thrown up by algorithms. Instead, companies - particularly the ones with significant market power - should be subject to greater transparency obligations and required to carry out human rights impact assessments as outlined below. In our view, the same reasoning should apply to navigation or 'discovery' services, i.e. they should not be penalised if their search engine algorithm returns illegal content but they should be transparent and explain to the public how their algorithm functions to return search results.

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

Our main concern is that 'enhanced' data sharing between online platforms and authorities could lead to a dilution of high standards of protection of personal data and the right to privacy so that data is used for other purposes or that the agreements allow national authorities to bypass more robust national procedures for getting access to data.

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

ARTICLE 19 is concerned that unduly high fines would have a detrimental effect on the protection of freedom of expression, particularly if the obligations imposed on online platforms involve targets for the removal or demotion of content or something equivalent. For this reason, ARTICLE 19 promotes Social Media Councils (SMC) as an alternative to regulatory oversight of social media platforms, though SMCs could co-exist within a co-regulatory framework to deal with content that is legal but harmful, i.e. that falls primarily within social media companies' community guidelines. For more details about the SMC, please see here: <https://www.cigionline.org/articles/social-media-council-bringing-human-rights-standards-content-moderation-social-media>

24 Are there other points you would like to raise?

3000 character(s) maximum

ARTICLE 19 further supports measures to promote media pluralism: when there is excessive market concentration, a small number of social media platforms act as gatekeepers of the flow of media content. In these circumstances, social media platforms should ensure that a diversity of media actors get their content distributed on their platforms. Regulators or competition authorities should be able to impose appropriate obligations, such as an equivalent to a must-carry duty in legacy media regulation in order to sustain media pluralism on social media platforms.

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

ARTICLE 19 believes that the above categories are generally fit for purpose. Nonetheless, we note that in recent years, there have been calls for social media platforms to be held liable for content in the same way as publishers. In our view, this is both a red-herring and profoundly mistaken. Social media platforms engage in three different types of activities: (i) they may produce content of their own, in which case the same liability should apply to them as publishers; (ii) they host content produced by third parties; and (iii) they distribute content, i.e. through the use of algorithms, they make certain types of content more visible and accessible to their users. This is often described as an editorial function or curation of content. However, it does not involve the production of content itself. As such, it should not attract any liability, save where the platforms have sufficiently intervened in the content such that it might be understood to be their own. Finally, it is important to remember that social media platforms such as Facebook, YouTube or Twitter operate at scale. It would be wholly impractical to hold them liable for the billions of pieces of content that go through their networks every hour.

Notwithstanding the above, there is one category that the DSA could potentially clarify, namely search services or linking liability, though in practice search services have often been equated with hosting.

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

ARTICLE 19 notes that a longstanding problem with Article 14 ECD (hosting immunity) is the lack of clarity surrounding what constitutes sufficient notice for the purposes of obtaining ‘actual’ knowledge of ‘illegality’. ARTICLE 19 has long argued that actual knowledge of illegality can only be obtained by a court order. To hold otherwise would be to accept that content is illegal simply because a third party, such as a copyright holder, said so.

In the alternative, we believe that the DSA could clarify the different types of notice and action procedures applicable to different types of content. In summary:

1. Notice-to-notice for private disputes (such as copyright or defamation): under this procedure, the

complainant or 'trusted flagger' would be required to give their name and set out in a notice why they believe that their rights have been infringed, the legal basis for their claim, the location of the allegedly infringing material, and the time and date of the alleged infringement. The hosting provider would be required to pass on the notice to the alleged wrongdoer (i.e. the content provider) as soon as practicable but no more than within e.g. 72 hours. The content provider would have a choice to remove the content or file a counter notice within a reasonable period of time (e.g. 14 days). Again, the hosting provider would be required to pass on the counter-notice as soon as practicable but within a maximum period of time (e.g. 72 hours). The complainant would then be given a period of time (e.g. 14 days) to decide whether they want to take the matter to court. The content would be removed following a court order. A hosting provider could be held liable for statutory damages if they failed to comply with their 'notice-to-notice' obligations, or if they failed to remove the content following a court order. By contrast, if the content provider failed to respond or provide a counter-notice within a given period of time, the hosting provider would lose immunity from liability. They could either remove the allegedly unlawful content or may be held liable for the content at issue if the complainant decides to take the matter to court or other independent adjudicatory body. In order to protect freedom of expression, any new notice-and-notice framework should also provide for penalties for abusive notices.

2. 'Notice and takedown' for allegations of serious criminality: under this procedure, a hosting provider would be required to takedown content when it receives a court order to that effect. In other words, they would be liable for failing to comply with such an order. In practice, this would mean that if law enforcement authorities believe that a piece of content should be removed and the matter is not urgent, they should seek a court order, if necessary on an ex parte basis. If, however, the situation is urgent, e.g. someone's life is at risk, law enforcement should be given statutory powers to order the immediate removal or blocking of access to the content at issue. However, any such order should be confirmed by a court within a specified period of time, e.g. 48 hours. The use of informal mechanisms - e.g. phone calls or emails requesting the host to remove content - should not be permitted.

By contrast, if hosting providers receive notice from an ordinary user about suspected criminal content, the host or platform should in turn notify law enforcement agencies if they have reasons to believe that the complaint is well-founded and merits further investigation. The host or platform may also decide to remove the content at issue as an interim measure in line with their terms of service. However, they would not be required to do so and failing to remove the content at issue would not attract liability.

The same process would apply to private bodies that work with law enforcement agencies and operate hotlines that individual internet users can call if they suspect criminal content has been posted online (see e.g. the Internet Watch Foundation in the UK or SaferNet in Brazil). In other words, the hotline would report the content at issue to both the host and law enforcement agencies. The host would use the same process that it uses for complaints from ordinary users, i.e. it would remain free to decide whether to remove content on the basis of its terms of service. The same model could be applied to other bodies, whether public or private, which receive complaints from the public concerning potentially criminal content online, or to notices issued by 'trusted flaggers' (see below for further details on trusted flagger programmes). Whichever option is pursued, it is important that the authorities are notified of any allegation of *serious* criminal conduct so that it may be properly investigated and dealt with according to the established procedure of the criminal justice system.

Finally, we note that the term 'expeditiously' could be clarified without imposing unduly short timeframes.

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

ARTICLE 19 notes that the current ECD regime presents risks to platforms since having certain tools in place has been deemed in some jurisdictions as giving them sufficient control over their networks for the purposes of 'actual knowledge' of illegality. Similarly, mandating upload filters or certain transparency requirements could imply that hosting providers have 'actual' knowledge of illegality on their respective platforms (for more details on the ways in which the ECD 'dis-incentivizes' service providers from taking certain proactive measures against illegal activities, see CDT, Positive Intent Protections: Incorporating a Good Samaritan principle in the EU Digital Services Act, July 2020: <https://cdt.org/wp-content/uploads/2020/07/2020-07-29-Positive-Intent-Protections-Good-Samaritan-principle-EU-Digital-Services-Act-FINAL.pdf>).

ARTICLE 19 believes that platforms and other tech companies should not be held liable simply because they adopt community standards, and use human moderators or other tools to enforce them (see e.g. Attorney-General opinion of 16 July in Joined Cases C-682/18 and C-683/18, especially paras. 132-168). In this sense, we support the adoption of a Good Samaritan rule that would encourage 'good' content moderation efforts made in good faith. In our view, failure to do so would prevent the adoption of innovative technical solutions and tools, such as demonetisation or the removal of certain platform features, that would strike a more proportionate balance between the protection of freedom of expression and tackling illegal or even 'harmful' content. At the same time, companies that use these tools should be subject to stringent transparency and due process requirements in relation to the way in which they use them. ARTICLE 19 also suggests that a multi-stakeholder forum such as the Social Media Council could facilitate the development of such technical or practical solutions in line with international standards on freedom of expression.

Similarly, companies should benefit from broad immunity from liability for the recommendations or suggestions made by their algorithms, even in circumstances where those algorithms recommend illegal content in response to content viewed by users. Whilst system developers and coders define the parameters within which 'algorithms' operate, they do not control or determine the outcome of these automated processes. Algorithms produce results from datasets in ways which are both complex and unpredictable. They are also both generally prone to making mistakes and unable to distinguish between lawful or unlawful content. Holding companies liable for every possible 'mistake' made by their systems would therefore be both unworkable and disproportionate. Insofar as liability deals with specific instances of illegality, it is also a poor instrument to address the systemic challenges thrown up by algorithms. Instead, companies - particularly the ones with significant market power - should be subject to greater transparency obligations and required to carry out human rights impact assessments as outlined below. In our view, the same reasoning should apply to navigation or 'discovery' services, i.e. they should not be penalised if their search engine algorithm returns illegal content but they should be transparent and explain to the public how their algorithm functions to return search results.

By contrast, we accept that companies should lose immunity from liability when they 'promote' - or 'optimise' the presentation of - illegal content in the advertisement section of their platform as a result of commercial agreements.

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

ARTICLE 19 believes that the concept of intermediaries playing a 'mere technical, automatic and passive' role retains some relevance, particularly as regards infrastructure providers ('mere conduit').

We note, however, that the CJEU's case-law in the L'Oreal v eBay case on the distinction between passive v active *hosting* has caused some confusion. Nonetheless, we support the Attorney-General's approach in his recent opinion of 16 July in the Cyando AG case (Joined Cases C-682/18 and C-683/18, especially paras. 132-168), which clarifies how this distinction should be understood in a lot more detail. In our view, the European Commission should rely on this Opinion to guide any clarification of the ECD and the concepts of 'active v passive' hosting.

Finally, we note that it is in the nature of the law to retain a degree of generality that is subsequently elucidated by the courts in the case-law. The DSA should aim to provide greater legal certainty and predictability but equally it must remain drafted so as to accommodate the development of new tools and services in future.

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 19 believes that governments must continue to prohibit general monitoring of content. Although it may be argued that monitoring merely enables companies to detect potentially illegal or 'harmful' content, in practice, mere detection is almost always coupled with removal or other types of actions reducing the availability of such content. This is deeply problematic given that content monitoring technology is not nearly as advanced as it is sometimes suggested. In particular, hash-matching algorithms and natural language processing (NLP) tools are currently incapable of distinguishing content whose legality may vary depending on context, such as news reporting or parody. Vast amounts of legitimate content may therefore be removed. Moreover, these technologies interfere with the privacy rights of users, as they require an analysis of individuals' communications.

In addition, if a law were to make immunity from liability conditional on 'general monitoring' or the adoption of 'proactive measures' or 'best efforts' to tackle illegal content - such as the EU Copyright Directive in the Digital Single Market, companies would inevitably err on the side of caution and remove content by default in order to avoid legal risks and enforcement costs. As noted by scholars, this could lead to platforms only allowing pre-screened speakers or using their Terms of Service to prohibit controversial content. It could also deter new market entrants from challenging incumbents.

At the same time, ARTICLE 19 recognises that 'specific' monitoring and removal of videos or other images that contain incontrovertibly unlawful child pornography, i.e. the depiction of sexual activity such as penetration between a child and an adult, may be compatible with the rights to freedom of expression and privacy. We do so given the gravity of the conduct at issue and the fact that this type of content can reliably

be recognised as unlawful regardless of context. We do not, however, agree that such specific monitoring obligations should be applied to any other kind of content.

Finally, we note that insofar as companies may well use automated filters on a voluntary basis, the use of these tools, particularly by the largest companies, should be both transparent and subject to human rights impact assessments, including their error rate and whether they render large quantities of information inaccessible. In our view, this would be consistent, *mutatis mutandis*, with the European Court of Human Rights' case-law on website blocking. In *OOO Flavus and others v Russia*, the Court has found violations of Article 10 ECHR (freedom of expression) in circumstances where the legal framework at issue did not require the authorities to ascertain that the blocking measure *strictly* targeted the illegal content at issue and had *no arbitrary or excessive effects*, including those resulting from the blocking of access to the entire website (at paras. 41-43): <http://hudoc.echr.coe.int/eng?i=001-203178>. Moreover, we believe that at a minimum the use of automated filters by private companies should include a 'human in the loop' for reviewing content moderation decisions.

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

ARTICLE 19 believes the DSA ought to be limited in its scope, including by reference to its subject-matter, the entities it seeks to cover and its geographical application:

- Focus on illegal rather than harmful content: we believe that any such framework should be limited to 'illegal' rather than 'harmful' content for the simple reason that 'harmful' content is an inherently vague concept. This makes it difficult to enforce, prone to abuse and open to challenge on legality grounds. In our view, legal content that is nonetheless prohibited under the community standards of companies should be subject to oversight by independent multi-stakeholder entities such as ARTICLE 19's proposed Social Media Councils. If "legal but harmful content" is included within the scope of the DSA contrary to our recommendations, then it should only impose transparency and due process requirements for the purposes of the company's enforcement of its community standards. The role of the regulator would therefore be limited to ensuring that companies' content moderation systems are sufficiently transparent and that users have clear and effective redress mechanisms available to them.
- Private messaging services and news organisations should be out of scope: we believe that the scope of application of any regulatory framework should be limited so that below the line comments on news sites and blogs are excluded. Equally, messaging applications and other private channels of communication should be out of scope. Regulators should not have the power to impose obligations on providers where such obligations would entail an unjustifiable interference with users' privacy rights, such as a weakening of end-to-end encryption or mandatory filters.
- Measures should not have extraterritorial application: we believe that the implementation of measures under such a new regulatory framework should be geographically limited to the country mandating such measures, consistent with international principles of comity and the proportionality principle under international human rights law. In other words, no one country should be able to issue orders to remove or otherwise restrict content that may be lawful outside its borders.

By contrast, we believe that the DSA should not include the following - non-exhaustive - types of obligations:

- A broad and undefined 'duty of care' to prevent an equally undefined notion of 'harm': in our view, such notions would be unlikely to pass the legality test under international human rights law. In practice, they

would both create legal uncertainty and give largely unfettered powers to regulatory authorities, which would be deeply problematic for freedom of expression.

- A general obligation to monitor content: a new framework should refrain from mandating general monitoring of content or measures that are substantially equivalent to it, such as mandating ‘best efforts’ or ‘proactive measures’ to tackle illegal content. Equally, such a framework should refrain from ‘nudging’ companies towards the adoption of such measures by framing them as purely voluntary or simply ‘recommended’, when in reality, failure to adopt them could lead to heavy sanctions.

- Unduly short timeframes: Internet companies should not be required to remove content within unduly short timeframes, particularly when the content at issue may give rise to difficult questions of interpretation, such as ‘hate speech’ or ‘terrorist’ content. Short removal timeframes do not incentivise companies to review notices sufficiently carefully. As such, they promote the wrongful removal of content and fail to protect freedom of expression. Moreover, as Facebook itself has noted, removals within short time frames can incentivise companies to allocate resources to removal of notices regardless of their severity or to focus on content simply because it has been posted in the last 24 hours rather than older content that may well be more deserving of attention.

- Compliance targets: lawmakers or regulators should not impose numerical compliance targets that could have the effect of encouraging companies to expand the definition of content they disallow on their platform in order to boost their compliance rate. We further note that insofar as lawmakers may be considering various metrics and thresholds to ensure compliance, they should consider the extent to which society can be expected to tolerate a degree of risk of harm online, as it does in the offline world.

- Obligation to cooperate or report illegal content: vague obligations to cooperate are problematic because they are typically difficult to enforce and could involve serious interference with users’ rights, such as access to user data by law enforcement without sufficient safeguards. They could also be counterproductive: obligations to report illegal content would likely give a strong incentive to companies to focus on notices of illegality regardless of severity.

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](#)






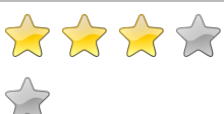

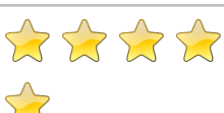



1 To what extent do you agree with the following statements?

	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 type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

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

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

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

Large user base	
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

In highly concentrated markets, the quality standards adopted by the gatekeepers, which include how much the service/products they offer guarantee data protection, free expression, non-discrimination and so on, become the quality standards of the entire market. In light of this, we believe that a criterion to use when assessing whether a firm holds a gatekeeping position is to look at whether the firm is able to set quality standards in the market. We call on the European Commission to always include in the concept of quality the impact that the product or service has on consumers' fundamental rights, and in particular on the rights to freedom of expression, privacy, data protection and non-discrimination.

Another characteristic which is relevant for determining the gatekeeping position is the fact that the firm is capable of making users' switching costs artificially high.

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

Regulators should perform an assessment that includes all characteristics that are relevant to identify a gatekeeping position. As mentioned, one of them is the capacity to set the quality parameters of a product or a service they provide in the market. To assess this capacity, regulators could rely on a consistent and well structured cooperation with other authorities, which have the relevant expertise and skills to perform such analysis (such as data protection authorities and consumer protection authorities). Those authorities could be called to provide assistance, for example in the form of opinions on the specific quality parameters of their concern (for example, privacy, non-discrimination etc.), which the regulator should be obliged to take into due account in its overall assessment of the existence of the gatekeeping position.

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

ARTICLE 19 believes that vertical and conglomerate integration are always likely to reinforce the gatekeeping role. To face this, the Commission should:

1. Impose vertical and functional separation when needed;
2. Impose adequate interoperability standards;
3. Impose access obligations on fair, transparent and non-discriminatory terms, and ban self-referencing practices;
4. Establish a presumption of negative impact of integration put in place by gatekeepers through mergers.

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

Social media companies with significant market power usually impose on individuals ToS that unduly and unfairly restrict their right to data protection and freedom of expression.

With regard to data protection, Facebook for example obliges users to consent to massive data collection and processing in order to use the service. It also obliges users to consent to Facebook combining all their personal data from different Facebook-owned services like Whatsapp and Instagram as well as from across the web into one single profile that's then sold to advertisers. Facebook practices with regard to data collection and data processing have been already subject to a variety of scrutinies, declarations of infringements and sanctions by competition and data protection authorities in the EU.

ToS do not have an impact on data protection only, they can also impact users' right to freedom of expression. Indeed, big social media companies profile their users and personalise the content they are exposed to based on profit-making criteria. Therefore, the variety and plurality of content each user is exposed to is artificially diminished by the personalisation exercise operated, in an opaque way, by the companies.

All in all, this platforms' behaviour results in an unfair and arbitrary reduction of the quality of the product offered to users, where the quality is marked by the degree to which their ToS protect fundamental rights. The effect of this behaviour is a substantial reduction of the welfare of consumers, which includes their actual enjoyment of freedom of expression, data protection and other fundamental rights on these platforms.

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

Massive data harvesting and profiling of users raise substantial data protection issues. In addition, they allow companies to monitor users' behaviour online, which makes it easier for the platform to lock them in.

Moreover, extremely detailed profiling leads to strong personalisation of content. This phenomenon has an impact on users' right to freedom of expression and information. Indeed, personalised content potentially reduces, based on profit-oriented criteria, the diversity of exposure of each user, without the latter being aware of it.

Political microtargeting raises specific challenges in relation to elections. On the one hand, ARTICLE 19 recognises that microtargeting can improve the efficiency of campaigns with limited resources and increase meaningful communication with voters on issues that are important to them. For this reason, smaller political parties and independent candidates can benefit from the use of micro-targeting by allowing them to access potential voters that they could not otherwise afford to target using traditional campaigning tactics; therefore, microtargeting tends to benefit new and heterogenous candidates and political parties at both extremes of the political spectrum, to the detriment of larger, incumbent parties that cater to a relatively stable and moderate voter base.

However, microtargeting can also create problems:

- Microtargeting raises questions in terms of individual autonomy and deliberation in a context where certain voters may not receive impartial information, and other demographic groups may fail to receive any information at all;
- Reliance on personal data may infringe data protection rights;
- Collecting data on ethnicity, religion, political affiliation, or proxies for sensitive information can lead to abuse;
- It can be difficult to detect, report and respond to problematic content such as misinformation and/or 'hate speech' that is only distributed to a small segment of users. This also raises the spectre of a political actor presenting conflicting policy positions to different groups, although there is no empirical evidence of this to date;
- It may become practically impossible to supervise the fairness of elections and sanction electoral infractions if the watchdogs of election campaigns, namely election authorities, NGOs, and journalists, are unable to monitor political communications, either because they lack technical access or the mandate.

ARTICLE 19 believes that new rules should ban "data opacity" for political ads and ask platforms for clear enforcement mechanisms for violation of their policies. Platforms should not be placed in the role of refereeing or mitigating aggressive political discourse and misinformation.

In addition, we call for enhanced transparency with respect to all political ad spending from relevant stakeholders, including political parties, tech companies, and third party advertisers. Political ads should be clearly distinguishable from editorial content, including news, whatever their form and including online, and clearly labelled with information about who paid for them. Furthermore, we support the use of digital ad databases to keep and publish all regulated ads, the amount of money spent on advertising, and the name of the person who authorised the ad, which should be accessible in a format that allows for bulk retrieval by researchers and policymakers.

Finally, we call for increased enforcement of GDPR rules. The GDPR requires clear affirmative consent to use of personal data that reveals political opinions (art. 9). In practice, consent to online targeted advertising is mostly obtained through cookie consent banners. However, it is unconvincing to suggest that this constitutes valid consent for political micro-targeting, given the opacity of the algorithms at issue and the blending of personal data from multiple sources.

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

3000 character(s) maximum

The imposition of unfair ToS exploits users and cements the platforms' position of market power. As such, platforms are ever less subject to the competitive pressure of alternative players, and lose incentives to innovate or to provide higher quality services to consumers.

This, in turn, reduces users' choices, as well as their bargaining power towards platforms. What is observed is that it is not demand to drive supply, as it is in healthy competitive markets, but rather the opposite.

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

Gatekeepers control access to the market and access to consumers. They make markets uncontestable, therefore limiting competition and reducing, when not eliminating, diversity and innovation. Doing so, they leave users without alternatives.

ARTICLE 19 is particularly concerned by the fact that if a company controls access to, for example, the social media market, it acts not only as "economic" gatekeeper, but also as "fundamental rights" gatekeeper, with particular impact on the rights to freedom of expression and privacy. This does not only manifest itself in this company's ability to dictate standard ToS for its users, but it also raises concerns where governments are able to pressure these gatekeepers into changing their ToS or implementing ToS in a way which is not compliant with fundamental rights (See also ARTICLE 19, Side-stepping rights: Regulating speech by contract, Policy Brief, 2018, available at <https://www.article19.org/wp-content/uploads/2018/06/Regulating-speech-by-contract-WEB-v2.pdf>)

Social media platforms represent one of the main channels which people in the EU rely on when exercising their right to freedom of expression. Therefore, allowing a single player to foreclose the social media market negatively affects the ability of citizens to exercise their freedom of expression.

Moreover, at community level social media platforms with market power can influence public debate, which raises issues in relation to diversity and plurality in the online environment.

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

The need for mandatory rules to address the gatekeeping role of large online platforms is grounded on a number of elements:

- 'Self regulation' adopted by gatekeepers has proved inadequate to keep markets open to competition and innovation, and to protect consumers' fundamental rights;
- Gatekeeping role is not necessarily caught by existing competition tools, which are triggered by the, usually higher, dominance threshold. Therefore, the phenomenon remains unaddressed by regulation;
- The gatekeeping role concerns, and should be assessed based on, not only economic effects, but also wider considerations with regard to the quality of the service/product;
- Gatekeepers jeopardise the vision of an open, free and democratic internet for all, therefore regulating them to minimise their impact on markets, individuals and society is a way to achieve various public policy objectives.

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 prohibitions need to address those behaviours and practices that typically lead to the creation of walled gardens, silos and closed ecosystems, such as those behaviors that raise barriers to entry for competitors and switching costs for consumers. For those conducts and practices, there should be a presumption of negative impact and gatekeepers should not be allowed to put them in place. The presumption should apply based on evidence collected by regulators on relevant cases.

In particular, practices and behaviours of large online platforms that impede access to the market for competitors, or that imply self-preferencing, should be prohibited.

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

ARTICLE 19 suggests an unbundling obligation for social media platforms' gatekeepers. Although hosting and curation activities are currently provided as a bundle by those platforms, this does not need to be the case, and it is not something irreversible. The bundle has a strategic economic value, and it contributes to lock in users and to raise barriers to entry to the market for potential competitors. This scenario is undesirable from a number of perspectives, and has an impact on competition, innovation, users' rights and, to a certain extent, also broader public objectives such as media plurality and diversity.

ARTICLE 19 calls for an ex ante remedy to address this situation: to oblige gatekeepers to unbundle hosting and content curation activities, and allow third parties to offer content curation to the platforms' users. We call for a form of functional separation, not a structural one. In addition, the platform that provides the hosting should remain free to offer content curation too.

The unbundling remedy should be designed to address the contractual layer (contractual agreements between the gatekeeper and the alternative players that provide content curation services to the platforms' users) and the technical layer (how to make this technically possible while ensuring data protection, consumer protection and security).

1. For the contractual layer, we suggest that gatekeepers provide access to competitors based on fair, reasonable, transparent and non-discriminatory grounds. We also suggest that gatekeepers should not be allowed to change the access conditions unilaterally in a way that nullifies competitors' efforts and investments.

2. For the technical layer, we believe the more efficient solution to be that gatekeepers should open a curation Application Programming Interface (API) to potential competitors. As such, the efficacy of the unbundling remedy is based on the adoption of interoperability solutions, whose details should be defined by the regulator, guided by independent experts with the relevant knowledge and in cooperation with the platform in order to deal with the substantial information asymmetries in the market. Indeed, as explained by

distinguished academic experts, various types of interoperability exist, and each of them could best fit different situations and needs (for example, Ian Brown, Interoperability as a tool for competition regulation).

The unbundling is less invasive or paternalistic than other current proposals to address challenges related to content curation, because it interferes only limitedly on digital platforms' freedom of economic activities and it empowers users to make their own choices, rather than imposing strict standards on the market. For more details about our unbundling proposal, see Annex to this Questionnaire.

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 unbundling is not a novelty in the history of economic regulation; on the contrary, it has been often used in network industries, and especially in the telecom sector. Therefore, we believe that there is no need for a new regulator in order to enforce it. What is needed, as mentioned before, is a proper system of cooperation and coordination among relevant authorities and bodies at the moment of assessing the gatekeeping position. In addition, as the unbundling should include technical provisions on interoperability, we call for the relevant regulator to make sure that it has the needed technical expertise, either internally or in the form of external independent support, to be able to shape the technical layer of the unbundling remedy.

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

We believe that the unbundling of hosting and content moderation activities is an efficient remedy for social media platforms that hold a gatekeeping role. Similar pro-competition remedies, which aim at vertical separation and access on fair, reasonable and non-discriminatory terms, could be tailored for gatekeepers in various markets.

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

As mentioned, ARTICLE 19 does not believe that there is the need of a new regulator in order to enforce the unbundling. Please see our answer to Q 8 above.

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

3000 character(s) maximum

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

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

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

3000 character(s) maximum

The unbundling remedy does not create any conflict with existing sector specific rules, which remain applicable. In addition, the remedy has to be shaped in a way that complies with relevant existing sector specific and horizontal rules, for example data protection and consumer protection. In other words, the remedy is an additional regulatory burden imposed on gatekeepers, which though leave untouched existing rules that already apply to them.

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

3000 character(s) maximum

The unbundling is a highly pro-competition remedy: it opens the market for content curation and relies on competition among players to deliver more choices and better-quality services to users. Therefore, on the one hand the unbundling contributes to solve the societal and human rights' challenges linked to content moderation. On the other hand, it is also capable of addressing the market failures such as excessive concentration in the market, barriers to entry, and other externalities created by the dominant platforms' behaviours that are not internalised and thus fall on individual users and on society, who pay the costs.

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

First, ARTICLE 19 notes that GDPR enforcement is still in its infancy in the EU and that a proper enforcement of its rules would, per se, promote competition, innovation and high data protection standards for EU consumers.

In addition, we believe that data portability principles established in the GDPR could be taken further and combined with interoperability principles in order, for example, to make users able to interconnect with people across competing platforms. These measures would make switching easier and provide incentives for new competitors to enter the market with better and innovative services. This could also lead to a variety of business models, with the possible appearance of business models that better guarantee users' data protection rights but also other fundamental rights.

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

ARTICLE 19 believes that the unbundling of hosting and content moderation suggested in our answer to question 6 would also have a positive impact on media pluralism on social media markets.

Indeed, the remedy would allow more content moderation providers in the market, and it would enable users to choose the one they prefer based, among others, on the criteria it uses for the curation and ranking of content. The presence of various providers, which will likely use different business models and different combinations of criteria for content moderation, would increase media diversity and plurality in the market.

One of the major advantages of unbundling as a tool to increase media diversity, is that the State intervenes in market dynamics and relies on healthy competition among players to ensure media diversity. Here, the metrics for pluralism are not set by a paternalistic State, but delivered by the market; it could be said that the State shapes the playing field but not the results of the game – which depend on the players' behaviours. With this in mind, unbundling appears to be one of the best placed solutions to achieve the public objective of media pluralism.

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

20 If other, please specify

3000 character(s) maximum

The regulator should be equipped with adequate resources to design, enforce and monitor unbundling remedies for social media platforms. It should also adopt mechanisms for efficient institutional coordination and cooperation, in various forms and at various layers, with relevant authorities and bodies. Among others, the cooperation should include the assistance mechanisms such as the issuing of opinions or advice, as well as the possibility to perform joint studies and investigations.

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

3000 character(s) maximum

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

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

23 Other – please list

3000 character(s) maximum

The regulator should have (i) the power to investigate the use of algorithms by platforms for the purposes of upholding their media diversity obligations, (ii) the power to investigate the use of personalised/micro-targeted advertisement systems, for instance in the context of elections or for the purposes of data protection legislation, and (iii) the power to impose sanctions (e.g. fines) for breaches of carefully circumscribed obligations under the DSA. By contrast, we note that regulators should not have powers to impose sanctions on platforms for failing to apply their own community standards, nor should they make decisions that would be akin to a determination of the legality of content.

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

3000 character(s) maximum

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

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

Option 5, which provides for the combination of ex ante rules and a new competition tool, appears the most effective solution to address not only the economic and market related issues arising in the online platforms ecosystems, but also the societal and human rights' challenges strictly interlinked with those issues.

Ex ante rules could be used to specifically address the market failures linked to gatekeeping, and to make markets contestable again. They could be also used to set market features (such as unbundling, vertical separation and interoperability) that reflect the vision of an open, free and democratic digital environment for the EU citizens and companies. In other words, ex ante rules, apart from fixing current market failures, could contribute to the achievement of other public policy objectives.

A new competition tool could complement this picture by adding a second layer of checks. Competition authorities could intervene ex post where the ex ante rules have not been sufficient to fix market failures and enable competition in the market.

ARTICLE 19 also draws attention to the fact that the combination of ex ante rules and a new competition tool should not result in an obstacle for the proper enforcement of other legal systems that online platforms ecosystems might be subject to. Data protection and consumer protection rules, among others, should remain applicable and be duly enforced. The existence of a shared regulatory space should not lead to the creation of incentives for under enforcement; on the contrary, cooperation measures should be in place to make sure that synergies are exploited and that coordinated intervention guarantees the achievement of all public objectives behind the shared regulatory space.

27 Are there other points you would like to raise?

3000 character(s) maximum

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

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

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

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

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

Online advertising

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

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

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

	% of ad space	% of ad revenue
Intermediated programmatic advertising 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

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

3000 character(s) maximum

ARTICLE 19 believes that to have meaningful transparency, at least this information should be made publicly available:

- Who published the ad
- Who paid for the ad
- Why any given individual is seeing this ad (categories, metrics, or other personal information used for the targeting)
- How much was paid for the ad
- A button to not be targeted again (a) from this publisher, (b) fr

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

Smart contracts

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

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



2 Please explain the difficulties you perceive.

3000 character(s) maximum

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

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

4 Please explain.

3000 character(s) maximum

5 Are there other points you would like to raise?

3000 character(s) maximum

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

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

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

Relationship with the platform and the final customer

1 What type of service do you offer through platforms?

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

2 Please explain.

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

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

- Yes
- No

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

- Yes
-

No

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

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

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

Situation of self-employed individuals providing services through platforms

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

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

- Yes
- No

15 Please explain.

The following questions are targeting online platforms.

Role of platforms

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

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

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

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

- Yes
- No

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

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

Rights and obligations

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

3000 character(s) maximum

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

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

25 Please explain.

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

- Yes
- No

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

3000 character(s) maximum

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

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

3000 character(s) maximum

The following questions are open to all respondents

Situation of self-employed individuals providing services through platforms

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

	1 (no improvements needed)	2	3	4	5 (substantial improvements needed)	I don't know / No answer
Earnings	<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?	
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

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 checked="" type="radio"/>	<input 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 checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Coordination and technical assistance at EU level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
An EU-level authority	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cooperation schemes with third parties such as civil society organisations and academics for specific inquiries and oversight	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other: please specify in the text box below	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

3 Please explain

5000 character(s) maximum

ARTICLE 19 is an international organisation that works to protect freedom of expression across the globe. In our experience, regulatory bodies tasked with oversight of media or social media companies generally lack independence resulting in violations of the right to freedom of expression. For this reason, ARTICLE 19 has advocated for oversight of social media platforms by an independent multi-stakeholder body such as social media councils (SMCs). Broadly speaking, SMCs would not concern themselves with illegal content but would ensure that the content moderation policies and practices of social media companies are in line with international standards on human rights, e.g. as reflected in a code of human rights principles for content moderation. SMCs would also deal with complaints about content decisions that have not been resolved through the companies' internal complaints mechanisms. They would operate in ways that are similar to press councils in the sense that they would not be able to impose fines or similar sanctions but would use remedies such as apologies or corrections in individual cases. SMCs would operate nationally but an international and/or regional cooperation mechanism could be envisaged. Our more detailed proposals are available here: <https://www.cigionline.org/articles/social-media-council-bringing-human-rights-standards-content-moderation-social-media>

Insofar as supervision of digital services is likely to fall in a shared regulatory space, and thus within the remit of various regulatory authorities (e.g. competition, consumer protection, data protection, media, anti-discrimination etc.), we believe that each competent national authority should deal with aspects that are relevant and consistent with its experience and overall expertise. However, cooperation mechanisms should be put in place to take advantage of synergies, eliminate wasteful duplications, better inform decisions and avoid conflicting ones, and to avoid fragmentation, capture and under enforcement. Various coordination tools could be put in place, among others:

- Consultations (in the form of advice, opinions etc.), either by law or jointly agreed by the authorities;
- Joint work, for example at the stage of investigation to secure information or at the stage of designing remedies;
- Joint policy making, to guarantee that the standards applied and the policies pursued are aligned.

We are less convinced of the need for cooperation mechanisms with swift procedures and assistance from national competent authorities across Member States in relation to decisions about the legality of content. Insofar as a regulatory authority may be issuing decisions that have an impact on freedom of expression, we believe that the scope of such a decision should be limited in its geographical scope to the Member States in which that regulatory authority has jurisdiction. We note, for instance, that EU Member States have different laws on 'hate speech' or strike the balance between freedom of expression and privacy differently. In our view, countries with a more restrictive approach to freedom of expression should not be able to impose their approach beyond their own borders. More generally, EU law should not require unanimity in the way in which national authorities or courts resolve the balance between competing rights (for an example of how this applies in the context of the right to be forgotten, see ARTICLE 19's submissions in the CNIL v Google case before the CJEU at paragraph 24 ff: <https://www.article19.org/wp-content/uploads/2017/12/Google-v-CNIL-A19-intervention-EN-11-12-17-FINAL-v2.pdf>).

We believe that some form of coordination at EU level is also needed. A structure similar to the European Data Protection Board could be useful. In addition, cooperation and coordination could also take place within existing fora such as the European Regulators Group for Audiovisual Media Services, the Body of European Regulators for Electronic Communications and the European Platform for Regulatory Authorities. The competence of any new network, as well as those of existing networks should be clearly identified to avoid duplication, and guarantee legitimacy and legal certainty. Similarly, we believe that engagement with external experts and civil society is important and should take place via possible observer status, participation in working groups and open consultations.

Finally, we remain sceptical that an EU-level authority would be best placed to deal with overall supervision and enforcement of the DSA. In our view, coordinational and technical level assistance at EU level would be more appropriate.

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

3000 character(s) maximum

ARTICLE 19 believes that competent authorities should provide maximum disclosure about their supervisory and enforcement activity, both in order to show how companies are being held accountable but also so that these authorities are held accountable themselves about their actions (or lack thereof). At a minimum, this should include:

1. an annual report including a list of infringement notices and sanctions or other measures imposed in accordance with the powers entrusted with the relevant competent authorities. Enforcement decisions should include the reasoning of the competent authority and be listed by type as appropriate. Annual reports should also include a section providing information about when and how the authority cooperated with other regulators and agencies. Annual reports should be transmitted to the national parliament, the government and other authorities as designated by Member State law. They should also be made available to the public, to the European Commission and to any other European body tasked with coordinating and/or ensuring proper cooperation in the area of platform regulation;
2. publication of a non-confidential version of all decisions, including reasons for those decisions;
3. publication of all information, including raw data and supporting documents, related to investigations or joint-investigations into company behaviours, subject to data protection or intellectual property law

requirements. The latter should be interpreted narrowly and this information redacted accordingly;

4. publication of guidelines, opinions, reports etc. adopted in the implementation of the DSA;

5. publication of rules of procedures, minutes of meetings, workplans etc of the competent authorities.

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

ARTICLE 19 believes that the regulator should be equipped with appropriate knowledge, expertise and skills in order to be able to address the specific challenges posed by social media platforms and other internet actors. In our view, this would be particularly important if the remit of a telecom and/or broadcast regulator is expanded to include a wide range of other companies whose industry culture and practices are very different from telecom and broadcast media companies. In practice, this is likely to include (but should not be limited to) technical skills and an understanding of the operation of content moderation at scale as well as knowledge and experience of fundamental rights, including freedom of expression, data protection and due process issues.

The regulator should be adequately resourced (both in terms of funding and Human Resources) in order to fulfil its role. Robust conflict of interest rules should be enforced, including cooling off periods, in order to prevent capture of regulatory authorities.

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

ARTICLE 19 is concerned that a drive to regulate digital services established outside the EU could be used or misused by other, less democratic countries, to impose their own requirements on global platforms. We are already seeing this with Turkey requiring companies with more than a million users in Turkey to establish an office locally and complying with draconian requests for removal of content. This was allegedly inspired by the NetzDG law in Germany.

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

3000 character(s) maximum

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

3000 character(s) maximum

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


3000 character(s) maximum





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

3000 character(s) maximum

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

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

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

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

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

3000 character(s) maximum

14 Are there other points you would like to raise?

3000 character(s) maximum

ARTICLE 19 notes that a degree of inconsistency in the implementation of substantive rules on e.g. 'hate speech' is to be expected as it reflects cultural differences across the EU about the weight being given to certain elements of context and societal norms. This is also likely to fall within the margin of discretion of regulatory authorities where applicable.

In addition, ARTICLE 19 believes that governments should ensure that Internet users have access to judicial remedies in order to challenge wrongful removal of content by platforms on the basis of their terms of service. Such remedies should include access to the courts but also to alternative dispute resolution mechanisms, such as e-courts or an ombudsman. In practice, governments should develop proposals for funding such mechanisms, including through a levy on social media platforms, for example. Moreover, consideration should be given to enabling various civil society groups, including those defending freedom of expression, to have standing to bring court proceedings, including class action lawsuits or in the alternative, allowing them to bring third-party interventions or provide expert opinions in cases raising freedom of expression issues.

This should be without prejudice to self-regulatory schemes, such as Social Media Councils, that would, among other things, enable users to challenge the content moderation decisions made by social media platforms by reference to an agreed set of principles, such as a 'Charter of Human Rights Principles for Content Moderation'.

Final remarks

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

1 Upload file

The maximum file size is 1 MB

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

2 Other final comments

3000 character(s) maximum

Useful links

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

Background Documents

[\(BG\) Речник на термините](#)

[\(CS\) Glosř](#)

[\(DA\) Ordliste](#)

[\(DE\) Glossar](#)

[\(EL\) á](#)

[\(EN\) Glossary](#)

[\(ES\) Glosario](#)

[\(ET\) Snastik](#)

[\(FI\) Sanasto](#)

[\(FR\) Glossaire](#)

[\(HR\) Pojmovnik](#)

[\(HU\) Glosszrium](#)

[\(IT\) Glossario](#)

[\(LT\) Žodynėlis](#)

[\(LV\) Glosārijs](#)

[\(MT\) Glossarju](#)

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

[\(PL\) Słowniczek](#)

[\(PT\) Glossrio](#)

[\(RO\) Glosar](#)

[\(SK\) Slovnk](#)

[\(SL\) Glosar](#)

[\(SV\) Ordlista](#)

Contact

CNECT-consultation-DSA@ec.europa.eu