Contribution ID: 3bf84cb8-bf72-43c6-9cc0-6925c5e7d16f
Date: 08/09/2020 18:10:10

Digital Services Act package: open public consultation

Fields marked with * are mandatory.

Introduction

The Commission recently announced a Digital Services Act package with two main pillars:

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

This consultation

The Commission is initiating the present open public consultation as part of its evidence-gathering exercise, in order to identify issues that may require intervention through the Digital Services Act, as well as additional topics related to the environment of digital services and online platforms, which will be further analysed in view of possible upcoming initiatives, should the issues identified require a regulatory intervention.
The consultation contains 6 modules (you can respond to as many as you like):

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

Digital services and other terms used in the questionnaire

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

How to respond

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

Deadline for responses

8 September 2020.

Languages

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

About you

*1 Language of my contribution

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

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

*2 I am giving my contribution as

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

*3 First name

Karolina

*4 Surname

Iwańska

*5 Email (this won't be published)

karolina.iwanska@panoptykon.org

*7 Organisation name

255 character(s) maximum

Panoptykon Foundation

*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

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.

26332554844-60

* 21 Country of origin

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

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

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

○ Burundi
○ Cambodia
○ Cameroon
○ Canada
○ Cape Verde
○ Cayman Islands
○ Central African Republic
○ Chad
○ Chile
○ China
○ Christmas Island
○ Clipperton
○ Cocos (Keeling) Islands
○ Colombia
○ Comoros
○ Congo
○ Cook Islands
○ Costa Rica
○ Côte d’Ivoire
○ Croatia
○ Cuba
○ Curaçao

○ Hong Kong
○ Hungary
○ Iceland
○ India
○ Indonesia
○ Iran
○ Iraq
○ Ireland
○ Isle of Man
○ Israel
○ Italy
○ Jamaica
○ Japan
○ Jersey
○ Jordan
○ Kazakhstan
○ Kenya
○ Kiribati
○ Kosovo
○ Kuwait
○ Kyrgyzstan
○ Laos

○ Northern Mariana Islands
○ North Korea
○ North Macedonia
○ Norway
○ Oman
○ Pakistan
○ Palau
○ Palestine
○ Panama
○ Papua New Guinea
○ Paraguay
○ Peru
○ Philippines
○ Pitcairn Islands
● Poland
○ Portugal
○ Puerto Rico
○ Qatar
○ Réunion
○ Romania
○ Russia
○ Rwanda

○ Tonga
○ Trinidad and Tobago
○ Tunisia
○ Turkey
○ Turkmenistan
○ Turks and Caicos Islands
○ Tuvalu
○ Uganda
○ Ukraine
○ United Arab Emirates
○ United Kingdom
○ United States
○ United States Minor Outlying Islands
○ Uruguay
○ US Virgin Islands
○ Uzbekistan
○ Vanuatu
○ Vatican City
○ Venezuela
○ Vietnam
○ Wallis and Futuna
○ Western Sahara

○ Cyprus

○ Czechia

○ Democratic Republic of the Congo

○ Denmark

○ Latvia

○ Lebanon

○ Lesotho

○ Liberia

○ Saint Barthélemy

○ Saint Helena Ascension and Tristan da Cunha

○ Saint Kitts and Nevis

○ Saint Lucia

○ Yemen

○ Zambia

○ Zimbabwe

*22 Publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

○ **Anonymous**
Only your type of respondent, country of origin and contribution will be published. All other personal details (name, organisation name and size, transparency register number) will not be published.

● **Public**
Your personal details (name, organisation name and size, transparency register number, country of origin) will be published with your contribution.

☑ I agree with the personal data protection provisions

I. How to effectively keep users safer online?

This module of the questionnaire is structured into several subsections:

First, it seeks evidence, experience, and data from the perspective of different stakeholders regarding illegal activities online, as defined by national and EU law. This includes the availability online of illegal goods (e.g. dangerous products, counterfeit goods, prohibited and restricted goods, protected wildlife, pet trafficking, illegal medicines, misleading offerings of food supplements), content (e.g. illegal hate speech, child sexual abuse material, content that infringes intellectual property rights), and services, or practices that infringe consumer law (such as scams, misleading advertising, exhortation to purchase made to children) online. It covers all types of illegal activities, both as regards criminal law and civil law.
It then asks you about other activities online that are not necessarily illegal but could cause harm to users, such as the spread of online disinformation or harmful content to minors.
It also seeks facts and informed views on the potential risks of erroneous removal of legitimate content. It also asks you about the transparency and accountability of measures taken by digital services and online

platforms in particular in intermediating users’ access to their content and enabling oversight by third parties. Respondents might also be interested in related questions in the module of the consultation focusing on online advertising.

Second, it explores proportionate and appropriate responsibilities and obligations that could be required from online intermediaries, in particular online platforms, in addressing the set of issues discussed in the first sub-section.
This module does not address the liability regime for online intermediaries, which is further explored in the next module of the consultation.

1. Main issues and experiences

A. Experiences and data on illegal activities online

Illegal goods

1 Have you ever come across illegal goods on online platforms (e.g. a counterfeit product, prohibited and restricted goods, protected wildlife, pet trafficking, illegal medicines, misleading offerings of food supplements)?

○ No, never
○ Yes, once
○ Yes, several times
○ I don’t know

3 Please specify.

3000 character(s) maximum

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

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

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

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

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

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

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

○ Yes

○ No

8 Please explain

3000 character(s) maximum

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

○ No, I do not think so

○ Yes, I came across illegal offerings more frequently

○ I don’t know

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

5000 character(s) maximum

Illegal content

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

○ No, never

○ Yes, once

○ Yes, several times

○ I don’t know

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

3000 character(s) maximum

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

3000 character(s) maximum

20 What actions do online platforms take to minimise risks for consumers to be exposed to scams and other unfair practices (e.g. misleading advertising, exhortation to purchase made to children)?

3000 character(s) maximum

21 Do you consider these measures appropriate?

○ Yes
○ No
○ I don't know

22 Please explain.

3000 character(s) maximum

B. Transparency

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

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

3 Please explain.

3000 character(s) maximum

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

○ Yes, I was informed

○ Yes, but not on every occasion / not by all platforms

○ No, I was never informed

○ I don’t know

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

3000 character(s) maximum

In order to gather more and more data about users and build more detailed user profiles that result in increased profits from targeted advertising, online platforms need to maintain users’ attention and maximise the amount of time they spend on the platform. To set this chain of events in motion platforms use algorithms to moderate, recommend, personalise and target content.

Despite this commonplace practice, most platforms do not offer any explanation at all in terms of why content has been recommended to users.

Some platforms have taken the initiative to present additional information for individuals on targeting of ads but such explanations are incomplete, misleading, and present insights only in terms of parameters selected by advertisers, ignoring the platform’s significant role in the process. For instance, empirical research [https://hal.archives-ouvertes.fr/hal-01955309/document] demonstrates that Facebook’s “Why am I seeing this ad?” feature shows only some of the reasons why a user was targeted with a particular ad, revealing non-controversial, most common and demographic reasons while hiding more granular and potentially sensitive criteria that were more relevant in the targeting process. Facebook shows only the attribute that is linked to the biggest potential audience. For example, if an advertiser selects two attributes — interest in “medicine” (potential reach of 668 million) and interest in “pregnancy” (potential reach of 316 million) — the user’s explanation will only contain “medicine” as the more common attribute [see more in our report “Who (really) targets you. Facebook in Polish election campaigns”: https://panoptykon.org/political-ads-report]

What’s more, explanations offered by platforms for sponsored content do not point the user to their specific personal data that was used in the targeting process or their sources. As a consequence, it is currently impossible for users to find out which of their characteristics or tracked behaviours were taken into account and how they were interpreted by a platform when matching them with a particular piece of content (sponsored or not).

In theory, the GDPR should be the right tool to curb these detrimental practices. Based on guidelines and opinions issued by the EDPB, we argue that users should be able to find out whether a particular piece of content has been personalised (targeted to them) and verify their personal data used for this purpose. In reality, there are certain aspects of the platforms’ power, like their algorithm-driven targeting abilities based on statistical correlations (i.e. not classified as personal data), which are not adequately addressed in the GDPR, as it remains difficult to track how exactly big data has been used to enrich individual profiles or inform individual decisions.

It is in this context that we propose additional transparency measures related to recommender / personalisation systems in response to question 20 in part 2.

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

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

3000 character(s) maximum

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

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

3 Please explain.

3000 character(s) maximum

The ad-driven business model incentivises platforms to curate information in ways that benefit advertisers, not users. Evidence shows that the ways Facebook, Twitter, and Youtube present content are designed to maximise engagement and drive up their quarterly earnings. This commercial logic that drives social media contributes to the spread and amplification of potentially harmful content and is detrimental to the quality of media, as it gives rise to clickbait, emotional and sensationalist messages. Citizens who are exposed to social media and low quality online content are more vulnerable to misinformation, profiling, and manipulation.

At the same time, algorithmic engines that drive content distribution across platforms are non-transparent and non-accountable which is particularly problematic in the case of amplifying disinformation and other forms of harmful legal content. These negative effects have already begun to spill over into various aspects of social life, including politics. A few parties to a large extent control which voices and which views will be seen, and which will not. Citizens who use large platforms in non-democratic regimes face a greater risk of government censorship and control.

We argue that in order to reduce (or at least prevent further escalation of) negative individual and societal effects caused by this business model, the DSA should address the source of the problem: platforms' targeting and personalisation capacities and lack of users' control over this process. We propose the following measures for achieving this goal:
-- enhanced transparency of content moderation, curation, and targeting, both for the public (incl. researchers and watchdogs) and for individuals,
-- effective tools to control the use of data that build on the provisions of the GDPR and include both default protections and granular data management settings,
-- minimum standard of interoperability as a precondition enabling the functioning of effective (i.e. independent from platforms' own business interests and their proprietary interfaces) tools for users to manage their data and shape their online experience (e.g. set own parameters for content personalisation).

The latter measure in particular has the potential to shift power over content curation that maximises engagement and amplifies harmful content (incl. disinformation) from platforms and their commercial clients to individual users and their trusted agents (e.g. nonprofits).

At the same time, if platforms choose to proactively remove content that their algorithms flag as "disinformation" or accounts that represent inauthentic behaviour, they should bear full legal responsibility for their own actions. In particular such actions should trigger legal obligations that will ensure transparency (e. g. revealing the logic behind algorithmic content curation) and accountability (e.g. due process for users affected by content moderation).

4 In your personal experience, how has the spread of harmful (but not illegal) activities online changed since the outbreak of COVID-19? Please explain.

3000 character(s) maximum

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

3000 character(s) maximum

D. Experiences and data on erroneous removals

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

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

5000 character(s) maximum

The information about the scale and impact of erroneous removals is impossible to track since online platforms do not share sufficient, comprehensive data in this respect. However, relying on our experience of an NGO looking into the problem of so-called 'privatised censorship', we are able to provide anecdotal evidence of erroneous removals, suggesting it is a widespread practice with serious implications for the protection of freedom of expression online.

Since 2019 we have been engaged in court proceedings before the Polish court against Facebook, supporting another NGO - The 'Civil Society Drug Policy Initiative' ('SIN') which had been arbitrarily blocked by the platform. In the lawsuit we demand restoration of access to SIN's removed pages and accounts as well as a public apology.

SIN conducts educational activities concerning harmful consequences of drug use as well as provides assistance to people who abuse such substances, including harm reduction activities. In 2018, without any warning or clear explanation, Facebook removed fan pages and groups run by SIN (the main page was followed by 16 000 users). The platform had characterized them as 'in violation of Community Standards' (no further justification was provided). SIN has attempted to use the mechanism provided by Facebook to challenge these removals, but to no avail (the platform never responded to the 'appeal'). Members of SIN still do not know which particular content was deemed as a violation of the Community Standards and for what reason. In January 2019, one of SIN's accounts on Instagram was also removed in similar circumstances.

Facebook was the key communication channel of the organisation, which SIN used to promote its activities and mission, to contact its volunteers, and to raise funds. Through Facebook, people using drugs could seek SIN's help. The removal of these pages, groups and accounts has made it considerably more difficult for the organisation to carry out its educational activities and other statutory tasks as well as reduced the reach of the published information and the possibility to communicate with a larger audience.

So far the court has delivered an interim measures ruling (not yet final) in which it has temporarily prohibited Facebook from removing fanpages run by SIN on Facebook and Instagram, as well as from blocking individual posts. The court has furthermore obliged Facebook to store profiles, fanpages and groups deleted in 2018 and 2019 so that – if SIN wins the case eventually – they can be restored together with the entire published content, (comments, followers etc). More information about the case: https://panoptykon.org/sinvsfacebook/en.

Other cases of unjustified Facebook removals we have identified based on media reports:
-- The Pulitzer-winning "Napalm Girl" photo and historical photograph of Jewish children during the WWII (for allegedly promoting nudity): https://www.theguardian.com/technology/2016/sep/09/facebook-deletes-norway-pms-post-napalm-girl-post-row https://techcrunch.com/2018/08/30/failbook/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=-D7WKrtSVuoUfvMeFsEUng
-- Press photos of the 2017 the Independence March – showing participants wearing symbols of extreme nationalist organizations (for allegedly promoting totalitarian symbols).
https://qz.com/1131572/facebook-is-still-struggling-with-the-difference-between-hate-speech-and-censorship/
-- Art such as The Origin of the World by Gustave Courbet or The Descent from the Cross by Peter Paul Rubens, both of which featured female nudes and other naked figures.

https://www.theartnewspaper.com/news/french-court-makes-mixed-ruling-in-courbet-censorship-case
https://www.artsy.net/news/artsy-editorial-facebook-censored-images-rubens-nudes
-- Pictures of people whose appearance is “unusual”: a picture of a plus size model and a former firefighter who lost his hair, eyebrows and ears in the line of duty.
https://www.theguardian.com/technology/2016/may/23/facebook-bans-photo-plus-sized-model-tess-holliday-ad-guidelines
https://www.telegraph.co.uk/news/2017/01/03/facebook-concedes-made-mistake-banning-image-bolognas-nude-statue/
-- The fan page of a popular British satirical magazine VIZ, famous for its provocative humour. In Poland YouTube removed one of the episodes of the satirical show concerning violence and discrimination against women. It was blocked because it allegedly incited violence against men.
https://www.theguardian.com/media/2016/feb/17/facebook-viz-magazine-page
https://krytykapolityczna.pl/kraj/youtube-algorytmy-przy-kawie-o-sprawie/

Some of these take downs have caused a public outcry, leading platforms to eventually restore the removed content. It is important to stress however that restoration of the content should not dependent on public /media pressure.

The following questions are targeted at organisations.
Individuals responding to the consultation are invited to go to section 2 here below on responsibilities for online platforms and other digital services

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

□ Yes, through regular transparency reports

□ Yes, through reports to a supervising authority

□ Yes, upon requests to public information

□ Yes, through other means. Please explain

□ No , no such reporting is done

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

□ Yes, data regularly reported by the platform, as requested by law

□ Yes, specific data, requested as a competent authority

□ Yes, through bilateral or special partnerships

□ On the basis of a contractual agreement with the platform

□ Yes, generally available transparency reports

□ Yes, through generally available APIs (application programme interfaces)

□ Yes, through web scraping or other independent web data extraction approaches

□ Yes, because users made use of their right to port personal data

□ Yes, other. Please specify in the text box below

□ No

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

3000 character(s) maximum

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

○ Yes

○ No

○ I don't know

13 How valuable is this information for you?

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

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

3000 character(s) maximum

The following questions are targeted at online intermediaries.

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

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

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

2 Please explain.

5000 character(s) maximum

3 What issues have you encountered in operating these systems?

5000 character(s) maximum

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

○ Yes

○ No

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

5000 character(s) maximum

6 Please provide information and figures on the amount of different types of illegal content, services and goods notified, detected, removed, reinstated and on the number or complaints received from users. Please explain and/or link to publicly reported information if you publish this in regular transparency reports.

5000 character(s) maximum

7 Do you have in place measures for detecting and reporting the incidence of suspicious behaviour (i.e. behaviour that could lead to criminal acts such as acquiring materials for such acts)?

3000 character(s) maximum

B. Measures against other types of activities that might be harmful but are not, in themselves, illegal

1 Do your terms and conditions and/or terms of service ban activities such as:

□ Spread of political disinformation in election periods?

□ Other types of coordinated disinformation e.g. in health crisis?

□ Harmful content for children?

□ Online grooming, bullying?

□ Harmful content for other vulnerable persons?

□ Content which is harmful to women?

□ Hatred, violence and insults (other than illegal hate speech)?

□

Other activities which are not illegal per se but could be considered harmful?

2 Please explain your policy.

5000 character(s) maximum

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

3000 character(s) maximum

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

5000 character(s) maximum

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

5000 character(s) maximum

6 Do you have specific policies in place to protect minors from harmful behaviours such as online grooming or bullying?

○ Yes

○ No

7 Please explain.

3000 character(s) maximum

C. Measures for protecting legal content goods and services

1 Does your organisation maintain an internal complaint and redress mechanism to your users for instances where their content might be erroneously removed, or their accounts blocked?

○ Yes

○ No

2 What action do you take when a user disputes the removal of their goods or content or services, or restrictions on their account? Is the content/good reinstated?

5000 character(s) maximum

3 What are the quality standards and control mechanism you have in place for the automated detection or removal tools you are using for e.g. content, goods, services, user accounts or bots?

3000 character(s) maximum

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

○ Yes

○ No

5 Please explain.

5000 character(s) maximum

D. Transparency and cooperation

1 Do you actively provide the following information:

□ Information to users when their good or content is removed, blocked or demoted

□ Information to notice providers about the follow-up on their report

□ Information to buyers of a product which has then been removed as being illegal

2 Do you publish transparency reports on your content moderation policy?

○ Yes

○ No

3 Do the reports include information on:

□ Number of takedowns and account suspensions following enforcement of your terms of service?

□ Number of takedowns following a legality assessment?

□

Notices received from third parties?

- □ Referrals from authorities for violations of your terms of service?
- □ Removal requests from authorities for illegal activities?
- □ Number of complaints against removal decisions?
- □ Number of reinstated content?
- □ Other, please specify in the text box below

4 Please explain.

5000 character(s) maximum

5 What information is available on the automated tools you use for identification of illegal content, goods or services and their performance, if applicable? Who has access to this information? In what formats?

5000 character(s) maximum

6 How can third parties access data related to your digital service and under what conditions?

- □ Contractual conditions
- □ Special partnerships
- □ Available APIs (application programming interfaces) for data access
- □ Reported, aggregated information through reports
- □ Portability at the request of users towards a different service
- □ At the direct request of a competent authority
- □ Regular reporting to a competent authority
- □ Other means. Please specify

7 Please explain or give references for the different cases of data sharing and explain your policy on the different purposes for which data is shared.

5000 character(s) maximum

The following questions are open for all respondents.

2. Clarifying responsibilities for online platforms and other digital services

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

	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)	Yes, only by larger online platforms	Yes, only platforms at particular risk of exposure to illegal activities by their users	Such measures should not be required by law
Maintain an effective ‘notice and action’ system for reporting illegal goods or content	○	●	○	○
Maintain a system for assessing the risk of exposure to illegal goods or content	○	○	○	●
Have content moderation teams, appropriately trained and resourced	○	●	○	○
Systematically respond to requests from law enforcement authorities	○	○	○	●
Cooperate with national authorities and law enforcement, in accordance with clear procedures	●	○	○	○
Cooperate with trusted organisations with proven expertise that can report illegal activities for fast analysis ('trusted flaggers')	○	○	○	●
Detect illegal content, goods or services	○	○	○	●
In particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law	○	○	○	○
Request professional users to identify themselves clearly (‘know your customer’ policy)	○	○	○	○

Provide technical means allowing professional users to comply with their obligations (e.g. enable them to publish on the platform the pre-contractual information consumers need to receive in accordance with applicable consumer law)	○	○	○	○
Inform consumers when they become aware of product recalls or sales of illegal goods	○	○	○	○
Cooperate with other online platforms for exchanging best practices, sharing information or tools to tackle illegal activities	○	○	○	●
Be transparent about their content policies, measures and their effects	●	○	○	○
Maintain an effective ‘counter-notice’ system for users whose goods or content is removed to dispute erroneous decisions	●	○	○	○
Other. Please specify	○	○	●	○

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

5000 character(s) maximum

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 of 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. This is 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

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

5000 character(s) maximum

In principle we believe that law should refrain from imposing a general obligation on intermediaries to prevent reappearance of illegal content by applying automatic re-upload filters. Imposition of such measures can likely only be achieved by filtering all content in the platform in search of specific previously identified unlawful items, which is questionable in the context of prohibition of general monitoring obligation (Article 15 of the e-commerce directive). At the same time we are aware of harmful implications of, for example, organized hate campaigns that rely on widespread copying and republishing of the content once removed from other places. Therefore, in order to support victims of such organized campaigns, we believe that introduction of an obligation to apply re-upload filters could be taken into consideration in very specific circumstances (as an exception to the general rule prohibiting its use) and given certain conditions are met, such as:
-- only with respect to very specific content (not 'similar' content)
-- only after the illegal nature of the content has been established by the court
-- only with regard to most harmful categories of the illegal content (such as hate speech or incitement to violence)
-- only with respect to some intermediaries (big platforms with high risk or widespread republishing of illegal content).

In addition to this, it would be essential that the law contains: appropriate safeguards against over-removals (see Q7 in Section II), as well as against abuse of algorithm-driven tools (see Q6 in Section II).

6 Where automated tools are used to detect illegal content, goods or services, what opportunities and risks does their use present as regards different types of illegal activities and the particularities of the different types of tools?

3000 character(s) maximum

According to our experience measures deployed to distinguish legal from illegal content turn our particularly ineffective when the decision seems to be taken solely by an algorithm (and not made/reviewed by a human). Algorithms perform badly at understanding and assessing the context in which content is produced, notably cultural, linguistic and social norms. Because of their contextual blindness or, in other words, inability to understand users' real meaning and intentions, automated tools often flag and remove content that is completely legitimate. This applies also to the application of imperfect image recognition tools that are used to assess photographs (here is an example of such a misjudgment by Facebook: https://www.facebook.com

/Panoptykon/photos/a.164613726035/10156016526621036/?type=3). As consequence online platforms overly relying on the use of automated identification and removal tools tend to record higher rates of wrongful take-downs.

In this context it is extremely important to stress that the use of automatic tools to assess the legality of the content (irrespective of whether it is mandated by law or it is platforms' own initiative) should be possible only provided that a number of safeguards are in place, such as due process and independent oversight of content moderation decisions (see also Q7 in section II) as well as safeguards against abuse of algorithm-driven tools (see Q17 in Section I.C and Q6 in section II for more information).

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

In terms of question a, digital services established outside the Union should fall under the DSA just as much as those established inside the Union.

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

Intermediaries that do not host but only cache or transmit user-uploaded content (such as DNS services, cloud fronting services and peer-to-peer messaging services) should not be held responsible for the content they transport. Web hosts, CDNs and other cloud storage providers that host user-uploaded content should only be held liable for that content if they refuse to act upon a valid court order in which content stored on their system has been declared illegal. We see the need for a fast-track court procedure in such cases.

Digital services acting as online intermediaries should not be required to proactively search for or remove content that has not been declared illegal by a court. Digital services are not in a position to arbitrarily decide which content is illegal or harmful or not. Requiring (or encouraging) them to exercise this power undermines the institutional and legal order of our democracy and cements the quasi-monopolistic position that many of these operators already occupy today.

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

A key role in tackling illegal activities online belongs to law enforcement authorities. In order to perform their duties effectively, they need to be well staffed and trained to find, properly document, and where appropriate prosecute illegal online activity without violating the fundamental rights of third parties, particularly their right to privacy and the freedom of expression.

The DSA should create a strong, effective and cross-border enforcement mechanism for oversight over platforms' own activities in tackling illegal content. Any oversight authority should be allowed and empowered to verify the functioning and legality of content moderation algorithms, the way platforms deal with content-related complaints, and the processes in place to do so in respect of people's fundamental rights.

Civil society can play an important role in creating public awareness and exposing illegal practices, but it should not be expected to act as a replacement for the responsibilities of competent authorities. In order for civil society to be able to perform this role, platforms must be required to offer a high standard of transparency of their content-related practices, in particular by publishing basic documentation (incl. results of human rights impact assessments) of algorithms they use to tackle illegal content. We encourage the European Commission to create a support system (e.g. grants) for civil society organisations to investigate platforms' practices, incl. publicly available HRIAs, in order to identify and flag potential abuses.

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

Legal content should be protected on the basis of freedom of expression. The law should not require platforms to proactively search for and remove content that is contested or harmful according to the platform' s own definition. If platforms engage in such activities on their own initiative, they should bear full legal responsibility for that. In particular such actions should trigger legal obligations that will ensure transparency (e.g. revealing the logic behind algorithms involved in flagging and removing harmful content) and accountability (e.g. due process for users affected by content moderation). The DSA should prescribe that such activities and the terms of service governing them must always be appropriate, proportionate, and transparent to users. Users need to be able to understand in clear language under which rules a given platform operates, how to abide by those rules, and be offered the right to effective remedy if their content is removed, including the possibility to contest the removal before an independent body in the user's jurisdiction and in the language that the user speaks.

We argue that platforms' gatekeeper power in defining what is harmful or not should be limited. Large online platforms should be required to enable users to protect themselves against unwanted legal content independently of platforms' curation algorithms. For that aim:
-- users should have a right to exercise fine-grained control over what they see – that control should override any business interest a platform may have in distributing certain content. This includes a right for users to opt out of content personalisation without any justification and a requirement for platforms to obtain users' explicit consent for targeting of sponsored content;
-- the DSA should mandate a minimum standard for protocol and data interoperability that is a precondition for the emergence of new tools that would allow users to shape their own online experiences independently of arbitrary content curation rules enforced by platforms.

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

5000 character(s) maximum

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

	1 (not at all necessary)	2	3 (neutral)	4	5 (essential)	I don't know / No answer
Transparently inform consumers about political advertising and sponsored content, in particular during election periods	○	○	○	○	●	○
Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with user complaints	○	○	●	○	○	○
Tackle the use of fake-accounts, fake engagements, bots and inauthentic users behaviour aimed at amplifying false or misleading narratives	○	○	●	○	○	○
Transparency tools and secure access to platform data for trusted researchers in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it	○	○	○	○	●	○
Transparency tools and secure access to platform data for authorities in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it	○	○	○	○	●	○
Adapted risk assessments and mitigation strategies undertaken by online platforms	○	○	●	○	○	○

Ensure effective access and visibility of a variety of authentic and professional journalistic sources	●	○	○	○	○	○
Auditing systems for platform actions and risk assessments	○	○	○	○	●	○
Regulatory oversight and auditing competence over platforms’ actions and risk assessments, including on sufficient resources and staff, and responsible examination of metrics and capacities related to fake accounts and their impact on the manipulation and amplification of disinformation.	○	○	○	○	●	○
Other (please specify)	○	○	○	○	○	○

13 Please specify

3000 character(s) maximum

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

3000 character(s) maximum

International human rights law puts very strict requirements for the conditions under which states can restrict freedom of expression and information (such as the principles of legality, necessity and proportionality, legitimacy). According to Article 15 of the European Convention of Human Rights, in emergency situations, states can derogate from their obligation in relation to freedom of expression and information but must justify such derogation by meeting two essential conditions: (1) the situation must amount to a public emergency that threatens the life of the nation or war; and (2) the state must have officially proclaimed that state of emergency and notified other countries through the Secretary General of the Council of Europe. In addition, every measure must be strictly required by the exigencies of the situation.

For these reasons, any cooperation between authorities and digital services that effectively restricts freedom of expression and information may only take place if conditions described above are fulfilled and should be regulated in a binding law.

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).

						I don't know /

	1 (not at all necessary)	2	3 (neutral)	4	5 (essential)	No answer
High standards of transparency on their terms of service and removal decisions	○	○	○	○	●	○
Diligence in assessing the content notified to them for removal or blocking	○	○	○	○	●	○
Maintaining an effective complaint and redress mechanism	○	○	○	○	●	○
Diligence in informing users whose content/goods/services was removed or blocked or whose accounts are threatened to be suspended	○	○	○	○	●	○
High accuracy and diligent control mechanisms, including human oversight, when automated tools are deployed for detecting, removing or demoting content or suspending users' accounts	○	○	○	○	●	○
Enabling third party insight – e.g. by academics – of main content moderation systems	○	○	●	○	○	○
Other. Please specify	○	○	○	○	●	○

16 Please explain.

3000 character(s) maximum

Beyond content moderation and transparency best practices, platforms should give their users finegrained control over what they see by enabling users to switch off personalisation without the need for any justification.

Users should also be able to actively curate their own content, which enhances personalisation. One way to achieve it is to open content-curation services/tools for competition and enable independent operators (with their own models and algorithms) to plug-in. That way, users could, for instance, receive a non-curated message stream or timeline from their social network and combine it with a third-party curation software offered by, say, a newspaper, European tech company, or civil society organisation they trust. We explain this proposal, together with minimum interoperability requirements that are a precondition to enable this sort of user control over content curation, in our responses to Section III of this consultation and the attached document.

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

Such fundamental rights violations can arise from two sources: either the behaviour of platforms users who upload illegal content or the behaviour of platforms themselves consisting in distributing content (sponsored or not) with the use of algorithms that prioritise certain content over another, reinforce biases, and are optimised to extract more data from people spending increasing amounts of time on a platform, thus enabling platform operators and other digital services to further improve their analytical and targeting capabilities.

Therefore we argue that measures to address the risks of violations of fundamental rights should be twofold.

First, in terms of risks resulting from uploading illegal content, we argue that it is vital to protect an updated limited liability regime for hosting intermediaries with regard to user-generated content.

While we explain our position in detail in Section II of this consultation, key elements of the updated liability framework are:
-- an introduction of a workable notice-and-action system complemented by the rules of due process, which empowers people to notify intermediaries of potentially illegal online content and behaviour they are hosting. While those user notifications should not make intermediaries legally liable for a legality assessment they may make, it should oblige them to verify the notified content and reply to the notifier and – where appropriate – the content uploader, with a reasoned decision. The reply should always include clear information about the possibilities for legal redress as well as the reasoning behind an action taken by the intermediary regarding the specific piece of content.
-- effective legal redress: regular courts in most EU countries are overwhelmed with content moderation cases from big social media platforms. That is why we support the creation of a fast-track procedure, e.g. via specialised tribunals or independent dispute settlement bodies in EU Member States that are cheaper, faster, and more accessible for affected users to settle speech-related disputes with other users or with hosting intermediaries.

Second, in terms of risks posed by platforms' own actions with content we propose that platforms should bear full legal responsibility for what they do on their own initiative. To this end, we recommend an introduction of a comprehensive accountability and oversight framework for algorithms that affect individuals, communities or other market players, in particular algorithms used to moderate, curate, personalise, (de) rank and target both sponsored and non-sponsored content. Please also note that we use the term "content" in its broadest meaning, which encompassess all types of user-facing features that are subjected to targeting or personalisation. It includes both content uploaded by the platform's users (e.g. posts, adverts, offers from online sellers) and content generated by the platform itself (e.g. price determinations, recommendations).

Such a framework should include:
(a) accountability of algorithms used for personalisation and targeting of both sponsored and non-sponsored content, incl. mandatory human rights impact assessment, independent audits, and effective oversight (measures governing the use of AI systems, as they are not only relevant to platforms, should be regulated in a horizontal AI-regulation, rather than the DSA package),
(b) enhanced public-facing, general transparency measures that reveal non-personal information to anyone interested (incl. researchers and regulators) and have the potential to expose platforms' and advertisers' practices for public scrutiny,

(c) individual transparency, which aims at explaining the targeting and personalisation process in particular cases and helping users understand why they are confronted with particular content.

This framework is comprehensively explained in detail in the attached document. We also describe relevant aspects of proposed measures in our responses to specific questions in this consultation form: for measures aimed at enhancing transparency and accountability of online advertising, please refer to our responses in Section IV; for measures aimed at algorithms used for personalisation of non-sponsored content please refer to question 20 in this Section.

18 In your view, what information should online platforms make available in relation to their policy and measures taken with regard to content and goods offered by their users? Please elaborate, with regard to the identification of illegal content and goods, removal, blocking or demotion of content or goods offered, complaints mechanisms and reinstatement, the format and frequency of such information, and who can access the information.

5000 character(s) maximum

19 What type of information should be shared with users and/or competent authorities and other third parties such as trusted researchers with regard to the use of automated systems used by online platforms to detect, remove and/or block illegal content, goods, or user accounts?

5000 character(s) maximum

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

5000 character(s) maximum

Algorithms that are widely used by platforms to (de)rank, personalise, recommend and target content are non-transparent and non-accountable. Although major online platforms have increased the transparency in some areas of their functioning (such as content and reach of adverts or their policies on content moderation), they continue to avoid offering any meaningful explanation of or insights into their targeting and personalisation machineries, both for the public (incl. researchers and regulators) and for affected users.

In theory, consistent enforcement of the GDPR should be the right tool to curb these detrimental practices. In practice, algorithm-driven targeting abilities based on statistical correlations (i.e. not classified as personal data) are not adequately addressed in the GDPR which leads to the following challenges in the context of recommender systems:
(1) Big data, understood as observations about people that result from statistical correlations, feed into algorithmic data processing and influence outcomes, which are experienced by individual users (e.g. the type of content that is recommended to them). At the same time it remains difficult to track how exactly big data has been used to inform individual decisions.
(2) Limitations of Article 22 of the GDPR: this provision regulates only fully automated decisions that produce

legally binding or other significant effects for an individual. In consequence, it can hardly be used to ensure user's control over content personalisation. While effects of personalisation are experienced by an individual, it is very difficult to "single out" a data processing operation that relates to a given individual because for marketing purposes users are "packed" into broader groups and categories.

It is in this context that we propose that large online platforms that personalise content (incl. newsfeed, recommendations, personalised offers, personalised pricing) should be subjected to specific transparency and accountability measures.

In terms of accountability of algorithms used for personalisation/recommendations online platforms should:
(1) perform mandatory Algorithmic Impact Assessments for algorithms that have significant impact on individuals, communities or other market players,
(2) publish the results of the assessment, regardless of the level of impact,
(3) when high impact is established, submit the assessment for independent external review (by a certified body) and notify the oversight authority whose role could be modelled on Article 36 GDPR regulating the process of data protection impact assessments,
(4) in any case platforms should present a general explanation to the public of how these systems work.

In order to design these measures in the most effective way, the European Commission should initiate a stakeholder engagement process. Specifically, the Commission should leverage stakeholder input to determine:
(a) audit criteria against which to assess systems; and
(b) appropriate auditing procedures of examination and assessment against these
criteria.

Both criteria and procedures should be further developed following a multi-stakeholder
approach that actively takes into consideration the disproportionate affect ADM systems have on vulnerable groups and solicits their participation. We therefore ask the Commission and Member States to make available sources of funding aimed at enabling participation by stakeholders who have so far been inadequately represented.

We recognise that accountability and transparency measures, related to the use of AI systems that affect humans, are not specific to large online platforms. As such they should be introduced in a horizontal regulation on AI rather than in the DSA package. Please refer to our response to consultations of the White Paper on AI for a comprehensive transparency and accountability framework for AI systems:
https://panoptykon.org/sites/default/files/stanowiska/panoptykon_ai_whitepaper_submission_10.06.2010_final.pdf

In terms of transparency measures aimed at explaining personalisation for individuals in their particular circumstances platforms should be required to make the following information available for each piece of personalised/recommended content:
(1) individual explanation of the personalisation process: users should have access to reasons why they are presented with a recommendation or another piece of content, including (but not limited to) personal data taken into account;
(2) sources of personal data used for personalisation by the platform (e.g. users' activity on the platform, its subsidiary, external website, information obtained from a data broker),
(3) GDPR legal basis and purpose of processing of personal data,
(4) indication and explanation of the optimisation goal pursued by the platform, e.g. engagement.

Please refer to the attached document for more details.

21 In your view, is there a need for enhanced data sharing between online platforms and authorities, within the boundaries set by the General Data Protection Regulation? Please select the appropriate situations, in your view:

- □ For supervisory purposes concerning professional users of the platform - e.g. in the context of platform intermediated services such as accommodation or ride-hailing services, for the purpose of labour inspection, for the purpose of collecting tax or social security contributions
- □ For supervisory purposes of the platforms' own obligations – e.g. with regard to content moderation obligations, transparency requirements, actions taken in electoral contexts and against inauthentic behaviour and foreign interference
- □ Specific request of law enforcement authority or the judiciary
- □ On a voluntary and/or contractual basis in the public interest or for other purposes

22 Please explain. What would be the benefits? What would be concerns for companies, consumers or other third parties?

5000 character(s) maximum

23 What types of sanctions would be effective, dissuasive and proportionate for online platforms which systematically fail to comply with their obligations (See also the last module of the consultation)?

5000 character(s) maximum

Financial sanctions should follow the example set by the GDPR. In addition the DSA should provide for behavioural remedies such as the ability of the regulator to impose interoperability,due dilligence and other procedural requirements on large platforms' operators, as well as explicit prohibitions. Please refer to our responses in Section III for more information.

24 Are there other points you would like to raise?

3000 character(s) maximum

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

The liability of online intermediaries is a particularly important area of internet law in Europe and worldwide. The E-Commerce Directive harmonises the liability exemptions applicable to online intermediaries in the single market, with specific provisions for different services according to their role: from Internet access providers and messaging services to hosting service providers.
The previous section of the consultation explored obligations and responsibilities which online platforms and other services can be expected to take – i.e. processes they should put in place to address illegal activities which might be conducted by users abusing their service. In this section, the focus is on the legal architecture for the liability regime for service providers when it comes to illegal activities conducted by their users. The Commission seeks informed views on hos the current liability exemption regime is working and the areas where an update might be necessary.

2 The liability regime for online intermediaries is primarily established in the E-Commerce Directive, which distinguishes between different types of services: so called 'mere conduits', 'caching services', and 'hosting services'. In your understanding, are these categories sufficiently clear and complete for characterising and regulating today's digital intermediary services? Please explain.

5000 character(s) maximum

For hosting services, the 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

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

That depends on the interpretation of the current provisions. In light of the interpretation presented by the EC in its 2017 Communication on tackling illegal content hosting intermediaries may be indeed exposed to a higher risk of liability if they decide to be more active in addressing illegal content proactively, which may disincentivize them to take such proactive measures. On the contrary, analysis of the national jurisprudence suggests that taking proactive measures in many cases would not lead to hosts losing the benefit of the liability exemption under the Article 14 of the e-commerce directive (however the domestic case law in this respect is not entirely consistent: In Poland there have been cases in which courts decided that the application of voluntary moderation measures by the platform led to obtaining "actual knowledge" and losing the protection of Art. 14 of the E-commerce directive.). Therefore, even though in general we believe that hosting platforms do not need extra incentives to take proactive measures (especially the big tech companies that, under the existing legal framework, are constantly scaling up technologies supporting moderation anyway) this question (i.e. hosting providers' liability when they undertake proactive measures) should be clarified for the sake of legal certainty.

At the same time, in principle, hosts should be free to apply ‘voluntary’ moderation activities on their platform without having to bear negative consequences of such a policy (in particular they should not be treated in a less favourable way than the ones not taking these measures). Therefore the sole fact of voluntary content moderation should not equal to ‘having actual knowledge’ about the illegal content and should not trigger ‘automatic’ liability in case when eventually a piece of such content is overlooked.

For those two reasons (legal clarity and ‘freedom’ to apply ‘voluntary’ moderation), adding the so called ‘Good Samaritan’ clause to the existing legal framework could be taken into consideration, provided however certain conditions are met. First of all, on the one hand, law must contain other incentives for hosts to tackle illegal content as they are an important component of the battle with online abuses (such as for example ensuring effective execution of their liability in case they do not take any action following up upon a receipt of an effective notice). On the other hand, “Good Samaritan” clause has some significant disadvantages as it could encourage excessive takedowns on the intermediary's own initiative, providing platforms with even more arbitrary power to remove content. This may lead to increasing volume of erroneous, unjustified removals, fuelling so called ‘privatised censorship’ (which, even in the absence of “Good Samaritan” defense, is already a widespread problem - see Q1 in Section I.D) and thus threatening freedom of expression online. Therefore the introduction of a ‘Good Samaritan’ clause has to be balanced with developing at the same time appropriate safeguards against such over-removals. These safeguards include in particular creating internal mechanisms (“due process” and transparency measures) which will ensure that platforms’ decisions are made in a transparent and non-arbitrary manner (including transparency of algorithms used for content management) as well as the possibility for users to have the final removal decisions of platforms verified by an independent external body (e.g. court). Please see more details in our response to question 7.

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

We consider the distinction between ‘active’ and ‘passive’ intermediaries to be outdated, incompatible with the current digital services landscape and therefore believe it should be abolished.

With an exception of mere conduit services (which should not have any ‘duty of care’ or secondary liability anyway), almost all modern online intermediaries are active to some degree, adopting more and more innovative approaches to attract or engage users. Maintaining the distinction between ‘active’ and ‘passive’ intermediaries creates interpretation controversies which result in lack of clarity as to which intermediaries may benefit from liability exemption. As a consequence this may incentivize them to take cautionary approaches which may foster over-removals.

Thus the Digital Services Act should rather focus on the particular types of services an intermediary offers as well as on the strict enforcement of legal obligations such as transparency, privacy and data protection. Liability exemption should apply under the simple condition that the hosting provider is not the creator of the content and has no knowledge about its illegal or infringing character (and acts upon obtaining such knowledge) [see: https://www.law.kuleuven.be/citip/blog/active-vs-passive-hosting-in-the-eu-intermediary-liability-regime-time-for-a-change/].

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

Yes, the prohibition of any general monitoring obligation is one of the cornerstones of a successful internet regulation. General monitoring consists of indiscriminate verification and control of all the online content or behaviour hosted on intermediaries’ systems for an unlimited amount of time and thus requires the mandatory use of technical filtering tools against all users. This would have very serious implications for freedom of expression (very his risk of over-removals) and right to privacy.

Therefore we believe that the concept of prohibition of general monitoring obligations should be maintained as a general rule. However, in case any derogations or limitations to that rule are introduced or if a platform implements general monitoring on its own initiative, it is essential that they are accompanied by sufficiently strong guarantees preventing the abuse of general monitoring tools, such as:
(1) mandatory human rights impact assessment of automatic content moderation tools complemented by independent audits and notification to an oversight authority (please see our response to Q17 in Section IV for more details on this procedure)
(2) the right to human intervention
(3) transparency rules (users should be able to understand the criteria according to which the filtering operates)
(4) due process rules (please refer to our response to Q7 for details).

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

Any content regulation solutions should address both a problem of effective countering of harmful content but also a problem of possible over-removals (in other words: any intermediaries' obligations facilitating effective fight with harmful content should be accompanied by measures preventing overblocking). The current regulations do not include any effective safeguards as regards the latter. The DSA should therefore ensure the following safeguards are in place:

(A) Online platforms should create internal mechanisms (‘due process’) which will ensure that their decisions are made in a transparent and non-arbitrary manner. In particular:

(1) A user whose content was removed should receive an explanation stating the reasons for the decision, including:

(i) Identification of the content that it deemed unacceptable;
(ii) A reasoned statement identifying the clause of the Community Standards that was breached;
(iii) Information on how the particular piece of content was identified as potentially abusive and how it was assessed (e.g. whether it was notified by another user, or whether it was “caught” by an automatic filter;

whether the decision to remove the content was made by a human moderator or by an algorithm);
(iv) Information concerning what the user can do if he or she disagrees with the platform's assessment.

This would allow each user not only to dispute the objections raised by a platform, but also to avoid similar situations in the future.

(2) Users should have a possibility to effectively appeal from the platform's decision.
(i) In order to be able to effectively challenge a decision, each user should have the opportunity to present arguments in their "defence".
(ii) The user's appeal should be considered by persons who were not involved in the making of the original decision and it should be carried out within a clearly pre-determined timeframe.

(3) All the moderation procedures mentioned above should be described in a transparent manner and be easily accessible to users (e.g. clearly resulting from the platforms' terms of service), so that everyone can easily check them and enforce their "rights".

(4) Online platforms should be legally obliged to publish transparency reports regarding their content moderation practices.

(B) In addition to internal 'due process' mechanisms users should have the possibility to have the final decisions of platforms verified by an independent external body, such as a court of law.

If a user believes that the removal of his or her content by a platform was wrong and that he or she had no real opportunity to defend himself/herself, he or she should be able to turn to the courts to analyse the matter and to order a revision of the decision (i.e. restoring the removed content or account). This has been recommended by, inter alia, the Council of Europe [see: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14]. It is the court, not a private company, that has the required authority to competently assess whether a particular statement exceeds the limits of free speech. This is why the courts should have the final say in these matters .It is important to stress however that the courts would have to be equipped with adequate resources that would guarantee their real availability and effectiveness in the context of the expected large number of such cases. An alternative may be therefore specialised tribunals or independent dispute settlement bodies in EU Member States that would be cheaper, faster, and more accessible for affected users to settle speech-related disputes with other users or with hosting intermediaries [as suggested by EDRi https://edri.org/wp-content/uploads/2020/04/DSA_EDRiPositionPaper.pdf].

Due process and independent oversight are particularly important when algorithms are used to assess and remove content due to the high risk related to these systems. In order to minimise this risk, platforms should be obliged to introduce transparency measures that enable users to understand when and how these systems work, how to challenge their decisions and in what cases they have been known to make mistakes. Please see our response to Q17 in Section I.C for more information.

III. What issues derive from the gatekeeper power of digital platforms?

There is wide consensus concerning the benefits for consumers and innovation, and a wide-range of efficiencies, brought about by online platforms in the European Union's Single Market. Online platforms facilitate cross-border trading within and outside the EU and open entirely new business opportunities to a variety of European businesses and traders by facilitating their expansion and access to new markets. At the same time, regulators and experts around the world consider that large online platforms are able to control increasingly important online platform ecosystems in the digital economy. Such large online platforms connect many businesses and consumers. In turn, this enables them to leverage their advantages – economies of scale, network effects and important data assets- in one area of their activity to improve or develop new services in adjacent areas. The concentration of economic power in then platform economy creates a small number of 'winner-takes it all/most' online platforms. The winner online platforms can also readily take over (potential) competitors and it is very difficult for an existing competitor or potential new entrant to overcome the winner's competitive edge.

The Commission announced that it 'will further explore, in the context of the Digital Services Act package, ex ante rules to ensure that markets characterised by large platforms with significant network effects acting as gatekeepers, remain fair and contestable for innovators, businesses, and new market entrants'.

This module of the consultation seeks informed views from all stakeholders on this framing, on the scope, the specific perceived problems, and the implications, definition and parameters for addressing possible issues deriving from the economic power of large, gatekeeper platforms.

The Communication 'Shaping Europe's Digital Future' also flagged that 'competition policy alone cannot address all the systemic problems that may arise in the platform economy'. Stakeholders are invited to provide their views on potential new competition instruments through a separate, dedicated open public consultation that will be launched soon.

In parallel, the Commission is also engaged in a process of reviewing EU competition rules and ensuring they are fit for the modern economy and the digital age. As part of that process, the Commission has launched a consultation on the proposal for a New Competition Tool aimed at addressing the gaps identified in enforcing competition rules. The initiative intends to address as specific objectives the structural competition problems that prevent markets from functioning properly and that can tilt the level playing field in favour of only a few market players. This could cover certain digital or digitally-enabled markets, as identified in the report by the Special Advisers and other recent reports on the role of competition policy, and/or other sectors. As such, the work on a proposed new competition tool and the initiative at stake complement each other. The work on the two impact assessments will be conducted in parallel in order to ensure a coherent outcome. In this context, the Commission will take into consideration the feedback received from both consultations. We would therefore invite you, in preparing your responses to the questions below, to also consider your response to the parallel consultation on a new competition tool .

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

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree	I don't know/ No reply
Consumers have sufficient choices and alternatives to the offerings from online platforms.	○	○	○	○	●	○
It is easy for consumers to switch between services provided by online platform companies and use same or similar services provider by other online platform companies ("multi-home").	○	○	○	○	●	○

It is easy for individuals to port their data in a useful manner to alternative service providers outside of an online platform.	○	○	○	○	●	○
There is sufficient level of interoperability between services of different online platform companies.	○	○	○	○	●	○
There is an asymmetry of information between the knowledge of online platforms about consumers, which enables them to target them with commercial offers, and the knowledge of consumers about market conditions.	●	○	○	○	○	○
It is easy for innovative SME online platforms to expand or enter the market.	○	○	○	○	●	○
Traditional businesses are increasingly dependent on a limited number of very large online platforms.	●	○	○	○	○	○
There are imbalances in the bargaining power between these online platforms and their business users.	●	○	○	○	○	○
Businesses and consumers interacting with these online platforms are often asked to accept unfavourable conditions and clauses in the terms of use/contract with the online platforms.	●	○	○	○	○	○
Certain large online platform companies create barriers to entry and expansion in the Single Market (gatekeepers).	●	○	○	○	○	○
Large online platforms often leverage their assets from their primary activities (customer base, data,	●	○	○	○	○	○

technological solutions, skills, financial capital) to expand into other activities.						
When large online platform companies expand into such new activities, this often poses a risk of reducing innovation and deterring competition from smaller innovative market operators.	●	○	○	○	○	○

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

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

Large user base	★★★★★
Wide geographic coverage in the EU	★★★★☆
They capture a large share of total revenue of the market you are active/of a sector	★★☆☆☆
Impact on a certain sector	★★★★☆
They build on and exploit strong network effects	★★★★★
They leverage their assets for entering new areas of activity	★★★☆☆
They raise barriers to entry for competitors	★★★★★
They accumulate valuable and diverse data and information	★★★★★

There are very few, if any, alternative services available on the market	★★★★☆
Lock-in of users/consumers	★★★★★
Other	☆☆☆☆☆

2 If you replied "other", please list

3000 character(s) maximum

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

3000 character(s) maximum

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

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

5 Other - please list

1000 character(s) maximum

Emerging issues

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

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

○ Yes

○ No

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

5000 character(s) maximum

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

5000 character(s) maximum

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

6 Do you encounter issues concerning commercial terms and conditions when accessing services provided by large online platform companies?
Please specify which issues you encounter and please explain to what types of platform these are related to (e.g. e-commerce marketplaces, app stores, search engines, operating systems, social networks).

5000 character(s) maximum

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

3000 character(s) maximum

The following questions are open to all respondents.

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

5000 character(s) maximum

1. Apple artificially prevents the installation of alternative software sources on its smartphones and tablets running iOS. Thereby, the company uses its market power as a device and operating system maker to control which software users can run on their own devices. While the security and privacy checks Apple undertakes on new apps is important, competitor app stores could be independently audited to ensure they provide equally effective checks.

2. Alphabet contractually requires smartphone makers to install the complete suite of proprietary Google apps (Gmail, Maps, Search, Play Services, etc.) if they wish to gain access to the Google app store (‘Play Store’), and prohibits the pre-installation of any competing apps (including competing app stores). Thereby, Alphabet uses its market power in operating systems to push its other services onto people’s phones and prevents any competitor from gaining a foothold in the market.

3. Facebook obliges users to consent to incredibly intrusive personal data collection and analysis in order to use its services. The company 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 marketed to advertisers (the German Cartel Office has ruled this to be an abuse of dominance). Facebook thereby uses its dominant position as a social network to cement its market power in the data and online advertising business.

4. Facebook makes it impossible for competing social networks to enable their users to interconnect with friends on Facebook. Thereby, the company abuses its market power and strong network effects to lock-in its users, to artificially prevent them from getting in touch with ‘the outside world’, and to suppress any potential competing social network from ever gaining a foothold in that market—most users are already taken by Facebook. Facebook’s forthcoming support for interoperability between its own messaging platforms, Messenger, WhatsApp and Instagram (with a combined 3.14bn users as of June 2020; see: Facebook Reports Second Quarter 2020 Results, 30 July 2020, at https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Second-Quarter-2020-Results/default.aspx), but not those of its competitors, is a further anticompetitive step.

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

Most platforms collect personal data from users based on platform and third-party website activity such as search history, location tracking, and interactions with friends. Despite data aggregation and display being a core component of their business models, their disclosure about how user data is collected and shared, and with whom, is not transparent. Further, platforms have historically placed the burden of privacy on users by requiring them to opt out of automatic data sharing and burying consent agreements in deceptively complex terms of service.

Ad-driven platforms use dark patterns and the power of defaults to obtain users' “consent” for omnipresent tracking and constant collection of their personal data, which by far exceeds what would seem justified by the nature of key services offered to users. These invasive practices make users “accept” excessive data collection and processing, without making them aware of what consequences it may entail.

In this process large platforms exploit not only on the data that users are willing (or forced) to share but – more importantly – on metadata and data inferred from their behaviour, such as observations on how they use the platform, what content they are exposed to, and how they react to it. Collected and generated masses of data are analysed with the use of algorithms and compared for meaningful statistical correlations. The task of these algorithms is to predict users' characteristics that they have never consciously revealed, such as their psychometric profiles, IQ level, addictions, beliefs etc., thus creating detailed profiles which are then offered to advertisers and used for personalising content.

Such observations, made by large platforms on the basis of big data (statistical correlations detected by algorithms), influence outcomes, which are experienced by individual users (e.g. the type of content that is presented to them). However, it remains very difficult for researchers and watchdog organisations to track how exactly big data has been used to enrich individual profiles or inform individual decisions. Looking from outside of the platform, it is hardly possible to “single out” a data processing operation that relates to a given individual.

Unsurprisingly, when confronted with access requests, none of the large platforms has revealed the full user profile that would include all data inferred about them. In response online platforms argue that inferred data is no longer personal (although it is contrary to the broad definition provided by the GDPR) or that inferred data constitute their trade secrets. As a result users have no control over the most valuable (and potentially sensitive) data that is collected or generated about them for marketing purposes.

Ad-driven online platforms do not perceive their users as clients. In this business model real service is offered to advertisers and it is their interest that shapes the design of “free” services. This is why all social media platforms are designed to maximize the amount of time users spend on their apps and sites to capture and monetize as much data from those user interactions as possible.The more time users spend on the platform, the more data they reveal; the more data they reveal, the more detailed their profiles become; the more detailed the profiles, the more revenues for platforms from selling targeted advertising.

Based on data collection practices described above large online platforms know more about citizens than political parties do. Political parties can commission a social survey or even buy customer data, but won't ever be able to profile the whole population and verify these opinions based on actual behaviour. This is especially pertinent in countries where political parties do not have access to electoral registries (as is the case in most EU countries),

Equipped with such data power, large platforms are not merely a passive intermediary between advertisers and targeted users. Platforms play an active role in the targeting process: their algorithms interpret criteria selected by advertisers and deliver ads in a way that fulfills advertisers' objectives. By doing so, platforms bear responsibility for negative effects of micro-targeting (discussed in Q13). For further analysis please refer to our report: https://panoptykon.org/political-ads-report

As discussed above, algorithms are used by large platforms to analyse personal data and target their users. The way these algorithmic engines work, however, is opaque and impossible to audit. For deep learning systems, explaining how individual decisions are reached may be extraordinarily difficult, if not impossible. Other decision-making algorithms, like the ones used to return Google search results or present Facebook's newsfeed, are considered proprietary and kept secret. This secrecy can help prevent manipulation, but it also comes at the cost of making it more difficult to detect discrimination.

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

3000 character(s) maximum

Example 1: Consumers cannot choose to install the software they like. They are dependent on Apple approving the respective app for its app store. The company has used this power in the past to ban certain types of apps in certain countries, and to ban all competing browser engines from its devices. As a result, all non-Apple browsers—like Mozilla Firefox, Google Chrome, and Brave—are forced to use Apple's own browser engine WebKit. But Apple could also use this power to slow down or prevent the publication of other apps that compete with its own services, like music streaming or messaging apps.

Example 2: Alphabet's behaviour hurts competition by foreclosing the smartphone app market to any other providers of similar apps/services. As a result, it becomes very hard—if not impossible—for competitors to have their search engines (like Qwant, Duckduckgo), email apps (likeFairEmail, Outlook), maps apps (like Maps.me, OSMand), or voice assistants(like Cortana, Alexa, Siri) pre-installed on smartphones running Android. This of course also severely limits user choice.

Example 3: Facebook's combining of personal data without user choice has an immense negative impact on consumer privacy rights and choice, as recognised by the German Cartel Office in its recent decision against the company. The more companies and digital services Facebook buys and operates, the harder it will be for people to use services without being forced to give up their personal data to Facebook. The situation is aggravated by the inclusion of Facebook tracking code into many major websites (such as the "Like" button). This code channels personal data to Facebook whenever someone visits a website, regardless of whether that person has a Facebook account or not.

Example 4: Facebook maintains several APIs that allow developers to interoperate with its core product. However, for developers to be able to access such APIs, it is necessary to agree to Facebook's platform policy, which prevents developers from offering apps that "offer experiences that change" Facebook, and to respect the "limits we've placed on Facebook functionality". Thus, Facebook deliberately refuses to allow competitors to interconnect or interoperate and prevents them from overcoming the network effects that cement Facebook's dominant position as a social network. If users were enabled to move their online lives to alternative networks without losing their connections on the dominant Facebook platform, a whole market would be liberated. Even new markets could be created by allowing startups to develop services on top of Facebook that interoperate with the platform. This would empower users to take advantage of additional functionalities and services (like a content moderation add-on or a better way to show and filter theFacebook timeline).

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

Algorithmic Bias and Digital Discrimination
Technology is not neutral, and algorithmic decision making can systematically treat groups differently in ways that can have real consequences, e.g. Carnegie Mellon study found that men searching for jobs were much more likely to be served ads for career-coaching targeting executive jobs than women were.

Election Interference and Political Influence
In recent years politically motivated actors have used platforms like Facebook to interfere with our elections. A 2016 study by Buzzfeed found that top fake election news stories generated more total engagement on Facebook than top election stories from 19 major news outlets combined. Although it is difficult to prove that political disinformation campaigns impacted election outcomes, it is clear that platforms can be leveraged to disseminate dangerous propaganda. The source of the political power of large platforms is their ability to wield opinion power or their ability to influence public discourse for their own purposes. The sheer possibility of the abuse of this immense power for one's own political goals is in itself a threat to any functioning democracy.

Misinformation, Disinformation and Echo Chambers
Unlike media companies, platforms are not ethically obligated to provide facts and unbiased reporting. As such, all content, regardless of its accuracy, is treated equally by platforms, leading to the mass circulation of false and inaccurate content. Moreover, platform ad revenue models are structured to favor content that gets the most clicks, views, and other engagement. Paired with precise targeting, this means platform users are purposefully exposed to content that they will likely agree, engage, and share with like-minded networks.This creates a social-validation feedback loop or echo chamber where individuals are only exposed to social and political content that reinforces their world view.

Privatisation of the Public Square and Censorship
As speech increasingly moves online, our venue for public discourse is owned and operated by corporate gatekeepers. Platforms that host and control public content are becoming quasi-governmental entities and are acting as arbiters and limiters of free speech, while remaining democratically unaccountable private powers.

Damaging Public Health
Ad-driven online platforms use algorithms to target content in a way that will maximize users' engagement and drive up their earnings. This commercial logic contributes to the spread and amplification of potentially harmful user-generated content (incl. clickbait, emotional and sensationalist messages). Recent studies have linked the use of platforms like Facebook, Snapchat, and Instagram to depressive symptoms in young adults by negatively comparing oneself to others on social media platforms. Targeted advertising has public health implications for vulnerable communities that are bombarded with advertisements for unhealthy food products.

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

The rise of online platforms' dominance in search, advertising, and social media has contributed to the crisis of traditional news media and quality journalism in a significant way. Now, as a primary channel for accessing news and information for an increasing share of the world, platforms are making content publishing and promotion decisions that are undercutting quality journalism by prioritizing “click-bait” and siphoning advertising revenue that might otherwise have supported traditional news media.

Despite their outsized role in our media ecosystem, social media platforms like Facebook and Twitter are not subject to advertising and content regulations that govern other media companies. Also, unlike media companies, platforms are not socially or ethically obligated to provide facts and unbiased reporting to the public. As such, all content, regardless of its accuracy, is treated equally by platforms, leading to the mass circulation of false and inaccurate content. The prevalence of misinformation and disinformation has severely undermined public credibility of news sources. Social media networks that reward virulence over veracity contributed significantly to this challenge.

Platforms dominate the online advertising revenue market and have taken critical funding away from traditional news media outlets to fund highly targeted ads that only platforms can offer. According to annual reports produced by the advertising industry itself, 85 percent of all new online advertising revenue is now funneled to either Facebook or Google. Without advertising revenue, newsrooms face serious challenges. Newsrooms have cut back on reporting staff, and some critical venues such as city hall and state governments go uncovered. To generate advertising revenue, news outlets may increasingly publish “sponsored stories” over quality content or be forced to put original stories behind a paywall. Either option would result in less quality news content reaching smaller audiences. Without media outlets committed to the public interest over revenue, the supply of fact-based, ethical reporting will most likely decline.

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 DSA should put in place rules, such as mandatory interoperability, that are able to limit the gatekeeper role that large online platform companies have acquired, as well as the resulting negative effects. There should be explicit obligations on gatekeepers to support interoperability, and duties to avoid measures that impede it. Just as in the European Electronic Communications Code, the European Commission should be given powers to designate technical standards that must be supported by specific gatekeepers.

Access to interoperability interfaces should not discriminate between different competitors and should not come with strenuous obligations. Interoperability interfaces, such as APIs, should be easy to find, well-documented, and transparent (The FRAND principles from telecommunications regulation could be adapted here.)

More specifically, new regulation for large platforms should mandate for:
(i) protocol interoperability, which would allow users to communicate with the platform in alternative ways (for example by sending a standard, DNT-like signal through their browser in order to express their tracking preferences or by choosing another client to manage their privacy settings);
(ii) data interoperability, which (on a basic level) can empower users to use their data rights (in particular the right to access, correct and move their own data) in a more effective way, without being limited by platforms' own interfaces.

Full protocol interoperability, when combined with data interoperability, would not only enable users to delegate a third-party software to interact with a platform on their behalf (e.g. send messages, like and comment on posts, read content) but also to federate selected features with competing platforms. Mandating for vertical and horizontal interoperability in the new regulation for large platforms will open the way for deep changes in the whole online ecosystem and certainly undermine large platforms' power to act as gatekeepers.

We expect that it would foster the development of competing services that not only have the ability to connect users on different platforms (e.g. with messaging services) but also function on the top of the large platform's ecosystem: complementing, modifying or replacing some of the platform's functionalities. In this scenario users of large platforms would not only be able to connect with pers on a different platform but also to curate their own newsfeed and define their own content filters using independent software. Mere existence of such competing services that are capable of modifying large platform's key functionalities would radically change power balance in an online environment.

Interoperability obligations for large platforms should be accompanied by strong privacy, security and non-discrimination rules. Users must be in full control of how, when and for what purposes their personal data is shared. The principles underpinning the GDPR must be protected.

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

New regulation for large platforms should prohibit practices and behaviours of large online platforms that impede access to the market for competitors, in particular:

(i) self-preferencing (i.e. nudging users to install applications owned by the platform operator when alternatives exist);

(ii) limiting access to the platform ecosystem (e.g. app store) for independent software providers, as long as these providers respect data protection and data security standards defined by the European law;

(iii) offering privileged access to own API to selected software developers or a more limited API (than available internally) to all potential competitors;

(iv) reserving their right to restrict or revoke access to API for any reason;

(v) ignoring signals communicated by their users (e.g. via their trusted agents) with the use of other protocols, as long as these protocols have been recognised by the European law or international standard setting bodies.

These behaviours and practices typically lead to the creation of walled gardens, silos and closed ecosystems. As such they create barriers to entry for competitors and switching costs for consumers. New regulation for large platforms should introduce the presumption of negative impact for such behaviours and practices (a sort of a black-list). This presumption should apply based on evidence collected by regulators on relevant cases.

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

In order to achieve minimum interoperability, large platforms should be obliged to:
1. adopt a standard protocol or publish their own protocol/API specification, through which third parties can interface with it;
2. ensure non-discriminatory access to this interface and allow all competitors to build independent services (i.e. applications and plug-ins) that complement, modify or replace some of the platform’s functionalities; in the case of social media platforms this obligation should lead to unbundling hosting and content curation, so that third parties can offer content curation to platforms’ users;
3. inform users about alternative applications and plug-ins whenever the platform prompts a user to install its own application (try new services);
4. maintain API for users and their trusted agents according to the standard defined by the regulator or specified in the regulation itself, which gives users real-time access to their own data and facilitates the exercise of their GDPR rights;
5. respect standard protocols (recognised by law or international standard-setting bodies) in communication with their own users (e.g. to manage privacy settings; set targeting preferences; access and transfer data)

and in communication with competing services (e.g. to federate newsfeeds or send messages).

These obligations will allow independent developers to ‘plug into’ large platforms’ ecosystems and pave the way for vertical and horizontal interoperability. Lack of compliance with these minimum interoperability requirements should be treated as unfair trading practice and the breach of EU law.

In addition to observing minimum interoperability requirements, large online platforms should be subjected to additional transparency and accountability measures. In particular these entities should be obliged to:
(1) report to national authorities or to the new European regulator data and parameters that enable ongoing assessment of their economic and social impact (e.g. user base, ad sales, turnover, presence in high-impact markets such as housing or finance); required data should be sent to via a dedicated interface;
(2) perform mandatory Algorithmic Impact Assessments for algorithms that have significant impact on individuals, communities or other market players (see section I.2 - Q20 and Section IV - Q17 for details).

Finally, the Commision should consider remedies tailored for individual platforms (ex ante rules). This toolbox should include:
1. data sharing obligations, e.g. to allow competitors to access behavioural data collected by the platform and /or statistical models developed on the basis of such data (if access to raw data would compromise users’ privacy) to the extent it is necessary for the development and provision of the competing service;
2. prohibitions and limitations when it comes to the use of personal and/or aggregated users’ data, e.g. prohibition of integrating 1st and 3rd party data for targeted advertising purposes.

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

When designing new rules for global players, it is essential to build in strong, effective and cross-border enforcement mechanisms. Unfortunately, past experiences show that it is unrealistic to expect effective, cross-border cooperation from a whole array of existing enforcement bodies, incl. data protection authorities (who struggle with the trans-national application of the GDPR), competition authorities (who decide case-by-case whether a given company has abused its dominant position), and media regulators (who are often politicised). Success of the DSA package will depend on the EU's ability to address these enforcement challenges and draw lessons from two years of cross-border application of the GDPR.

The DSA package should include the mandate for either an entirely new regulatory body or a new coordination mechanism for existing bodies to be established on the European level. This body or a group of bodies should be tasked with supervising the implementation and enforcement of the DSA package, in combination with other legislation that shapes the digital market, such as the GDPR. Therefore, regardless of the institutional solution selected by the European Commission, there will be the need for close cooperation between new regulation and the Data Protection Board.
While we don’t have strong opinions on how to shape a new regulatory body or a new coordination mechanism, we would like to reiterate that this institution or a group of institutions must be equipped with

strong monitoring and enforcement powers (incl. ability to perform unexpected controls and audits as well as legal mandate to issue high financial penalties and order structural measures).

At the same time new regulator should not be tasked with decisions that directly affect accessibility and legality of online content (e.g. reviewing content moderation decisions taken by large platforms), since such decisions should remain in the hands of independent judicial bodies or relevant national regulators (e.g. arbitration bodies or media regulators)

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

Specific regulatory intervention is necessary to address competition, consumer protection and fundamental rights issues. The digital market moves rapidly and therefore people and companies affected by the abuse of a gatekeeper position cannot wait until antitrust authorities have spent years to analyse and formulate theories of harm. The functioning and effects of the abuse of a gatekeeper position are sufficiently well studied to enable a regulator to step in and impose immediate remedies. Europe cannot wait another decade for investigations by DG Competition, with narrow decisions which are appealed by every avenue possible in the European courts by some of the world's richest companies, and even when successful fail to set broad precedents. Therefore new regulation for large platforms should empower the regulator to impose tailor-made remedies against their uncompetitive behavior.

Types of remedies applied in particular cases should depend on the business model and the conduct of a particular large platform. Therefore, at this point, we are not able to enumerate all types of possible remedies, which may become useful in particular cases.

However, we can indicate examples of remedies that would make a positive difference if applied to existing uncompetitive practices of the large platforms:
1) for large platforms that collect 1st party data (at times illegally) and combine it with 3rd party data in order to create granular marketing profiles (e.g. Facebook and Google's business model), it would be an adequate remedy to prohibit the combination of 1st and 3rd party data for targeted advertising;
2) for large platforms that engage in self-preferencing or other gatekeeping practices (examples of such practices are given above), it would be an adequate remedy to impose their vertical and/or functional separation (e.g. decoupling of the underlying network infrastructure from business operations and provisioning of services);
3) for large platforms that have built their dominant position (e.g. in behavioural advertising or electronic media market) on tracking and analysing users' behaviour over time, it would be an adequate remedy to give competitors access to statistical models developed on the basis of users' personal data and/or to raw data collected by the platform if it is deemed necessary in a specific case;
4) for social media platforms that act as gatekeepers it would be beneficial to mandate full interoperability,

which not only allows competitors to build new services based on large platform's infrastructure but also to federate different social networks and build services that interconnect users.

11 If you consider that there is a need for such dedicated rules, as referred to in question 9 above, do you think there is a need for a specific regulatory authority to enforce these rules?

- ○ Yes
- ○ No

12 Please explain your reply

3000 character(s) maximum

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

3000 character(s) maximum

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

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

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

3000 character(s) maximum

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

3000 character(s) maximum

Yes, both perspectives can and should be taken into consideration.

There are obvious important impacts of online platform market structures in areas of policy far from straightforward economic concerns. For example, a thriving and competitive market for independent news and journalism is essential for an effective democracy. While the business model of large platforms (based on maximising user attention and hence advertising revenues) has well documented negative side effects (including the amplification of disinformation, hate speech and extremism), interoperability could help build the counter powers and disperse opinion-forming power in the online ecosystem. Interoperability would allow European companies -- large and small -- to produce alternative tools for Europeans to connect to various online public squares, which would replace existing 'walled gardens' that are curated and controlled by large platforms.

However, the DSA should specify the objectives that a regulator is allowed to pursue when tackling negative social effects caused by the gatekeeper in question. Concretely, the regulator should not be able to impose remedies on a gatekeeper vaguely citing some "negative societal effects". The DSA should include a concrete list of such effects that would empower the regulator to act.

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

The DSA package offers the chance to correct shortcomings of the GDPR and to build further on its most promising provisions. In particular we reiterate the need to facilitate users' access to effective and transparent data management tools, which will support data portability as outlined in Article 20 GDPR (see attached document for detailed analysis of this problem and proposed solutions). We also argue that for data portability to work in practice there must be a competitive end-point to move data to. New regulation should therefore encourage and facilitate creation of such competitive platform infrastructure (eg. trusted data sharing spaces across the EU).

Going beyond the GDPR to address the negative social and economic impact of the large platforms, we would like to reiterate the need to open access to data controlled by these entities, so that this resource can serve non-commercial goals and enhance competition on the digital market.

In particular we propose that the DSA package:
(1) empowers the new regulatory authority to set mandatory European standards and protocols for data sharing (as discussed in our response to question 6 above), which will facilitate data sharing via users' trusted intermediaries, including third-party software;
(2) specify the right of large platforms' users to move their data to personal 'pod' in the European Common Data Space, where they can be further processed according to GDPR and serve other goals (incl. non-commercial);
(3) introduce mandatory data sharing regime for public-interest research purposes;
(4) introduce binding rules outlining who can directly access data or apply for access; what specific data can be accessed; how and by whom that data is to be gathered and checked before disclosure.

Because of the sensitive nature of certain types of data, there are legitimate concerns to be raised regarding threats to user privacy. The Cambridge Analytica scandal should serve as a cautionary tale, and any misuse of data by researchers would severely undermine the integrity of any transparency framework. New rules allowing for access to data (currently controlled by large platforms) must therefore be compatible with GDPR principles including (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimization;

(d) accuracy; (e) storage limitation and (f) integrity and confidentiality.

New legal framework for data sharing should give preference to users’ trusted intermediaries and make access to data conditional upon compliance with the GDPR. Granular data access should only be enabled within a closed virtual environment, controlled by the independent body. As was the case with the Findata framework, it is advisable for the Commission to consider testing key components of the framework in pilot phases.

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

3000 character(s) maximum

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

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

20 If other, please specify

3000 character(s) maximum

We observe that economic and societal issues that result from the growth of online platforms are complex and handling them requires a cross-sectoral approach, which may pose a challenge for existing regulators. Therefore it seems advisable to design a new regulatory body or at least a strong coordination mechanism for existing bodies (as discussed in our response to question 8 above).

If a new regulatory authority is created, it should be well equipped to exercise the following tasks:
(1) monitoring the digital market, competition, and openness of the internet in cooperation with competition authorities, consumer protection authorities and DPAs;
(2) monitoring large platforms’ behavior (including carrying out own investigations and analysing reports provided by the platforms on a regular basis);

(3) coordinating efforts of national competition authorities related to the digital market;
(4) supporting evidence-based national and EU policy making whenever it affects the digital market;
(5) acting on behalf of national authorities when requesting information from an online platform possibly infringing the DSA or other European regulations created to ensure competitiveness, consumer and data protection.

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

Regulatory oversight over large platforms acting as gatekeepers can be further facilitates by the following tools and requirements:
(i) introducing and enforcing common European standards for minimum interoperability (as discussed in our response to question 2 above);
(ii) introducing mandatory algorithmic impact assessments for these entities and related reporting obligations (as discussed in our response to question 17 in section IV);
(iii) introducing reporting obligations that will facilitate on-going monitoring of large platforms economic and social impact (specified in our response to question 6 above).

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

3000 character(s) maximum

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

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

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

3000 character(s) maximum

In order to respond to the abuse of a gatekeeper position in online platform markets, DG COMP or the new regulator should be empowered to use a New Competition Tool (addressing structural competition concerns). In addition, the DSA should provide the same regulator with powers to act on a case-by-case basis and address individually emerging uncompetitive practices.

If the DSA package were to be limited to a set of prohibited practices, coupled with transparency and reporting obligations for large platforms, we see the risk that dominant entities will correct their business models but we won't see structural changes in the digital market. Therefore tailored remedies for individual platforms are also necessary. Behavioural remedies and structural changes (such as decoupling of the underlying network infrastructure from business operations and provisioning of services, as discussed in our response to question 10 above) should come first, before ex ante rules can be effectively applied in order to prevent unfair practices from reemerging.

27 Are there other points you would like to raise?

3000 character(s) maximum

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

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

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

This section of the open public consultation seeks to collect data, information on current practices, and informed views on potential issues emerging in the area of online advertising and smart contracts. Respondents are invited to reflect on other areas where further measures may be needed to facilitate innovation in the single market. This module does not address privacy and data protection concerns; all aspects related to data sharing and data collection are to be afforded the highest standard of personal data protection.

Online advertising

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

○

Yes, always

○ Sometimes: but I can find the information when this is not immediately clear

● Sometimes: but I cannot always find this information

○ I don’t know

○ No

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

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

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

3000 character(s) maximum

4 As a publisher, what type of information do you have about the advertisement placed next to your content/on your website?

3000 character(s) maximum

5 To what extent do you find the quality and reliability of this information satisfactory for your purposes?

Please rate your level of satisfaction	☆☆☆☆☆

6 As an advertiser or an agency acting on behalf of the advertiser (if applicable), what types of programmatic advertising do you use to place your ads? What is their relative importance in your ad inventory?

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

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

3000 character(s) maximum

8 To what extent do you find the quality and reliability of this information satisfactory for your purposes?

Please rate your level of satisfaction	☆☆☆☆☆

The following questions are targeted specifically at online platforms.

10 As an online platform, what options do your users have with regards to the advertisements they are served and the grounds on which the ads are being served to them? Can users access your service through other conditions than viewing advertisements? Please explain.

3000 character(s) maximum

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

Algorithm-driven ad targeting, despite being the very source of platforms' power, remains highly opaque. Voluntary measures adopted by platforms aimed at increasing the transparency of this process are insufficient. Major online platforms have increased transparency of content and reach of adverts (by collecting relevant data in ad libraries) but they continue to avoid offering any meaningful explanation of or insights into their own role in the targeting process.

Except for GDPR rules that apply only to the processing of personal data in individual cases, there are no binding laws that would specify what kind of information related to ad targeting platforms should reveal and in what form. This makes it impossible to hold platforms to account as it is against their economic interests to reveal the inner workings of their targeting engines. While transparency on its own is not sufficient to limit platforms' excessive powers, we see it as a basic prerequisite for accountability.

Ad targeting normally involves third parties (advertisers) who initiate the targeting process, create their own messages, and choose the profile of their target audience. Despite this, platforms still play a key role at multiple stages of the targeting process: from data collection and analysis, which enables identifying users' attributes for advertising purposes, to optimisation of ad delivery. While advertisers do make their own choices, their choices have been shepherded by platforms and increasingly rely on data that was collected or inferred by them. A meaningful ad transparency framework should therefore cover actions of both advertisers and platforms.

A meaningful transparency framework should also distinguish between:
(a) public-facing, general transparency measures that reveal non-personal information to anyone interested (incl. researchers and regulators) and have the potential to expose platforms' and advertisers' practices for public scrutiny,
(b) individual transparency, which aims at explaining the ad targeting process in particular cases and helping users understand why they are confronted with a particular ad.

In terms of general transparency measures please refer to our answer to Q16.

On the individual level, the transparency framework should consist of two elements:
(1) explanation of the logic behind targeting that would enable users to understand what specific data and criteria were taken into account in their particular case;
(2) personal ad library - a database containing all ads that have been targeted at users and all advertisers who targeted them within a specified time (we propose 5 years). This database should not repeat information that is available in the public ad library but should contain relevant links (to the public ad library and individual explanations), thus making it easier for users to access information relevant for them.

Please refer to the attached document for more details.

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

3000 character(s) maximum

Platforms are not passive intermediaries between advertisers and users but play a key role that shapes the end result of targeting. They do so by:
(1) shepherding the choices that advertisers can select in the first place,
(2) using algorithms to determine which users fulfill advertisers' criteria (based on personal data collected by the platform itself and statistical analysis),
(3) optimising the delivery of ads (i.e. showing the ad to people who are more likely to respond to the ad in a way that the advertiser desires).

Therefore, a meaningful ad transparency framework should cover decisions made by both the advertiser and the platform.

The introduction of ad libraries has been a good step towards enhancing transparency of ads. However, the fact that platforms have full discretion in terms of whether to maintain ad libraries at all and what information should be made available, undermines the reliability and usefulness of this tool. Therefore we recommend that the DSA mandates an obligation for large platforms to maintain ad libraries, as well as specifies minimum requirements for information that ad libraries should reveal.

In terms of scope, ad libraries should include all ads, not only political ads (see more on why this should be the case and additional requirements for the latter category in Q19).

In terms of categories of information, ad libraries should contain at least:
(1) the content of the ad itself;
(2) *all* targeting criteria selected by advertisers for a particular ad, incl. optimisation goal selected by them and - if applicable - specification of seed audience used for lookalike targeting and indication of the source of data uploaded to a custom audience tool (such as newsletter list, website pixel), as well as information on A /B testing;
(3) information on the impact of an ad (the number of impressions that an ad received within specific geographic and demographic criteria, broken down by paid vs. organic reach).

Access to ad libraries should be possible via a regulated and programmable API, enabling continuous and automated collection of data. APIs that are currently offered by platforms have limited functionalities and have proved to be unreliable. While binding legislation might not be the best tool to shape the design of interfaces offered by platforms, it can formulate minimum technical requirements for their APIs.

In terms of platforms' role in the ad optimisation process publicly available information should include results of human right impact assessment performed for algorithms used for that purpose as well as a general, user-friendly explanation on how these systems work. Please refer to the next question for a proposed accountability framework for algorithms used for ad targeting.

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

3000 character(s) maximum

Meaningful accountability in the ad placement system should include accountability of algorithms used for ad targeting by the platform. The approach we propose is modelled on the GDPR provisions on data protection impact assessments but with important corrections based on two years of experience with the DPIA. Rules for AI systems, as they are not platform-specific, should be introduced in horizontal AI regulation.

All platforms that use algorithmic systems to target ads should be required to conduct human rights impact assessments of these systems. Further obligations (incl. independent audits) should depend on the level of impact established in the HRIA.

HRIAs should include:
(1) normative explanations of how the system was built (including steps that have been taken to ensure that the outcomes are unbiased and fair);
(2) key technical parameters, such as: loss function; formal fairness metrics; presentation of performance measurements; results of cross-validation (training/ testing splits) and any external validation carried out; presentation of confusion matrix (i.e. the table that provides the range of performance metrics);
(3) an assessment of the impact of these design decisions on (groups of) individuals.

When high impact is established:
(1) Independent external review of the system should be performed by a specialised review body (we support the direction of “prior conformity assessment” process outlined in the EC White Paper on AI). The report from the review should be annexed to the HRIA.
(2) After an external review is completed, the oversight body should be notified and provided with the HRIA and the review report, as well as any supporting documentation. The role of the oversight body could be modelled on Article 36 of the GDPR.

Regardless of the level of impact, HRIAs should be made available to the public in an easily accessible and machine-readable format. The document may be redacted but it should still offer meaningful insight into the HRIA process. Publication of HRIAs enables public debate on the quality of impact assessment and makes it possible for civil society or investigative journalists to identify/flag potential abuses. We don’t see another way to ensure that potentially dangerous uses of AI are not qualified as ‘low-impact’ or ‘low-risk’ by the developer/deployer and therefore escape any form of external review or public scrutiny.

We believe that this proposal addresses both the shortcomings of self-assessment and the risk of overloading public oversight bodies. Internal and external reviews should be combined with strong administrative measures (such as high financial penalties and decision to halt the deployment) if an entity fails to implement adequate measures to mitigate risks identified during HRIA.

More details: https://panoptykon.org/sites/default/files/stanowiska/panoptykon_ai_whitepaper_submission_10.06.2010_final.pdf

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

The concept of a “political” ad is highly ambiguous and difficult to enforce in practice. Major online platforms have shown that they struggle to identify political ads at scale. An independent study from Princeton [https://github.com/citp/mistaken-ad-enforcement/blob/master/estimating-publication-rates-of-non-election-ads.pdf] found many false positives and false negatives in Facebook’s U.S. Ad Library. Another study by ProPublica found unarchived ads on issues including civil rights, gun rights, electoral reform, anti-corruption, and health care policy. In December 2019, a bug in the UK archive caused almost all political ads from the preceding month to be deleted from the UK archive, massively disrupting research efforts. And the French government has observed that, “Facebook removed 31% of ads in the French library over the week of the European parliamentary elections, including at least 12 ads that were illegal under French law” [https://disinfo.quaidorsay.fr/en/facebook-ads-library-assessment#poor-data-integrity].

For these reasons we propose that basic transparency requirements for targeting should cover all ads. For researchers and institutions scrutinising political adverts, transparency of targeting for all adverts avoids the problems in agreeing on a controversial definition of “political issues.” Secondly, it is the only way to make sure that researchers and institutions are not missing anything, and that platforms’ rules are being enforced properly. In addition, commercial targeted advertising also creates many risks that may require intervention - especially on behalf of children and other vulnerable groups. Comprehensive transparency rules enable research into harmful commercial advertising (e.g. the sale of illegal or restricted products, the use of manipulative tactics, or discriminatory ad targeting), and are important from the perspective of consumer protection and data protection authorities.

At the same time, we acknowledge that a higher level of transparency regarding financing and engagement should be available for political or elections-related ads (see Q19). While we are not ready to offer a bullet-proof definition of political or election-related ads, we trust that it is possible to develop such a definition in a multi-stakeholder process, led by European institutions.

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

In addition to information on targeting and impact of ads, available in ad libraries for all adverts (see more details in our answer to Q16), the following information related to financing and engagement should be revealed for at least political or elections-related ads:
(1) the exact amount spent on the advertising campaign;
(2) information on who paid for the advert;
(3) engagements and interactions with the advert beyond viewing, such as numbers of “click-throughs” and “shares” of the advert.

We are conscious of the difficulties related to defining what constitutes a political or elections-related ad (see our response to the preceding question). At the same time we acknowledge that disclaimers that we propose above may be considered excessive by commercial actors, whose advertising budgets and tactics are not restricted by law. This extra level of scrutiny is justified in the case of political or election-related ads due to their sensitivity and potential impact.

In terms of users’ control over the process of targeting them with political ads, we argue that by default users’ behavioural data should not be used for this purpose. Platforms should be required to obtain explicit consent for showing users political ads (separately from consent for advertising in general).

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

Large online platforms that rely on advertising revenue have the unprecedented capacity to collect, process, and analyse vast amounts of data to optimise user experience and shape entire markets, including online content dissemination and online advertising. By some estimates, two advertising giants - Google and Facebook - control 84% of the global digital ad market. Large user base, which has grown as a result of network effects, generates endless streams of data, which feed platforms’ analytical capacity and their ability to attract commercial clients, who are willing to pay for the promise of (micro-)targeted advertising.

Online publishers willing to compete for users' attention and advertisers' money with major platforms are forced to play by their rules. First of all, with online platforms being one of the key channels of media content distribution, publishers are reliant on platforms' content dissemination algorithms that aim to maximise the time the user spends on the platform. This commercial logic is detrimental to the quality of media, as it gives rise to clickbait, emotional and sensationalist messages that provoke stronger reactions and increased engagement. Second of all, in an attempt to attract advertisers to their own websites, online publishers have to "accept" that they would share up to 70% of their advertising revenues with third parties that they engage to track users across the web and across devices [https://mediatel.co.uk/news/2016/10/04/where-did-the-money-go-guardian-buys-its-own-ad-inventory/].

At the same time, high profits generated by targeted advertising, maintained over time, allow Facebook and Google to invest in even better analytical tools and further secure their dominance on the advertising market, making online publishers fight a losing battle.

A comprehensive set of rules aimed enhancing transparency and accountability of online advertising on platforms that we explore in our responses to other questions and that include (a) exposing platforms' targeting practices, (b) introducing default protections and additional data management tools for users, and (c) mandating obligatory protocol and data interoperability, will in our view pave the way for deep changes in the whole online ecosystem and undermine large platforms' power to act as gatekeepers.
As a consequence, users (also with help from their trusted agents) could set their own preferences for content they want to see independently of platforms' content curation algorithms, which opens up space for media plurality and improved quality of content. In a situation where platforms' targeting power is limited, online publishers could explore ways of generating revenue that do not force them to share most of it with third parties or compromise their users' privacy, e.g. by looking at successful examples of implementing contextual advertising [see for example: https://www.ster.nl/media/h5ehvtx3/ster_a-future-without-advertising-cookies.pdf].

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

3000 character(s) maximum

For the purposes of this consultation it is useful to distinguish between advertising in closed platforms' ecosystems and advertising on the open web. The difference between these two advertising systems is that the latter relies on cross-site and cross-device tracking performed by a large number of intermediaries (also known as the ad tech industry), while platforms have exclusive control over the entire advertising process, from data collection and analysis to ad delivery.

Advertising on the open web is facilitated by online browsers that technically enable ad tech companies to install tracking cookies. Due to privacy concerns, browser operators have over the last few years increased default protections, e.g. Safari's Intelligent Tracking Protection or Firefox Enhanced Tracking Protection. These developments have pushed the advertising industry and online publishers to search for new ways of continuing monetising users' data (e.g. first-party cookies or new tracking technologies).

These trends have not remained unnoticed by Google - a company that apart from running a social media platform (YouTube) is a key intermediary in open web advertising (Google Authorized Buyers) and analytics (Google Analytics), and operates the dominant web browser (Google Chrome, with estimated 60% market share). In a move that shook the online advertising industry, Google announced that it would phase out support for all third-party cookies in Google Chrome by 2022. Instead, all user data would stay in the browser and would be controlled by Google for the purposes of ad targeting. What it means in practice is that Google – under the guise of protecting privacy – will turn its Authorized Buyers system into - yet another - walled garden at the company's disposal.

In a "post-cookie" world offered by Google the security of users' browsing habits would undoubtedly improve as they will be tracked and profiled not by hundreds of companies, but by one – Google. As a consequence, Google will monopolise data about people collected outside of Google's own services. Gathering a significant part of users' digital life under the umbrella of one company creates an unprecedented risk of influence and manipulation, that can be exploited both by commercial and political actors. It will also strengthen Google's power as the advertising hegemon and put any other company (including online publishers) under Google's thumb.

In this context, the DSA package is an opportunity to prevent such power consolidation from happening, in particular by introducing explicit prohibitions and obligations (such as minimum interoperability requirements) limiting the gatekeeper power of platforms and improved control tools for users to manage their data and actively shape their online experience. Please refer to Part III of the consultation and the attached document for more details.

Smart contracts

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

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

2 Please explain the difficulties you perceive.

3000 character(s) maximum

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

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

4 Please explain.

3000 character(s) maximum

5 Are there other points you would like to raise?

3000 character(s) maximum

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

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

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

Relationship with the platform and the final customer

1 What type of service do you offer through platforms?

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

2 Please explain.

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

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

○ Yes

○ No

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

○ Yes
○ No

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

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

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

Situation of self-employed individuals providing services through platforms

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

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

○ Yes

○ No

15 Please explain.

The following questions are targeting online platforms.

Role of platforms

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

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

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

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

○ Yes

○ No

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

○ Over 75%

○

Between 50% and 75%

○ Between 25% and 50%

○ Less than 25%

Rights and obligations

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

3000 character(s) maximum

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

□ The platform

□ The individual offering services through the platform

□ Others, please specify

25 Please explain.

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

○ Yes

○ No

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

3000 character(s) maximum

30 What measures do you have in place for ensuring that individuals offering services through your platform work legally - e.g. comply with applicable rules on minimum working age, hold a work permit, where applicable - if any?
(If you replied to this question in your answers in the first module of the consultation, there is no need to repeat your answer here.)

3000 character(s) maximum

The following questions are open to all respondents

Situation of self-employed individuals providing services through platforms

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

	1 (no improvements needed)	2	3	4	5 (substantial improvements needed)	I don't know / No answer
Earnings	○	○	○	○	○	○
Flexibility of choosing when and /or where to provide services	○	○	○	○	○	○
Transparency on remuneration	○	○	○	○	○	○
Measures to tackle non-payment of remuneration	○	○	○	○	○	○
Transparency in online ratings	○	○	○	○	○	○
Ensuring that individuals providing services through platforms can contact each other and organise themselves for collective purposes	○	○	○	○	○	○
Tackling the issue of work carried out by individuals lacking legal permits	○	○	○	○	○	○
Prevention of discrimination of individuals providing services	○	○	○	○	○	○

through platforms, for instance based on gender, racial or ethnic origin						
Allocation of liability in case of damage	○	○	○	○	○	○
Other, please specify	○	○	○	○	○	○

33 Please explain the issues that you encounter or perceive.

3000 character(s) maximum

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

○ Yes
○ No
○ I don't know

35 Please explain and provide examples.

3000 character(s) maximum

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

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

3000 character(s) maximum

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

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

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

3000 character(s) maximum

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

3000 character(s) maximum

40 Are there other points you would like to raise?

3000 character(s) maximum

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

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

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

Main issues

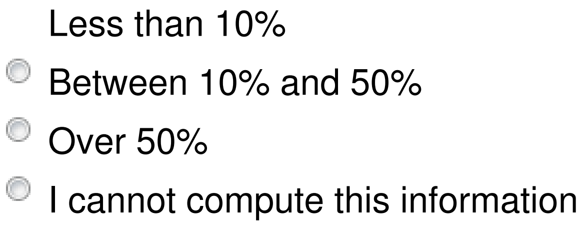
1 How important are - in your daily life or for your professional transactions - digital services such as accessing websites, social networks, downloading apps, reading news online, shopping online, selling products online?

Overall	☆☆☆☆☆
Those offered from outside of your Member State of establishment	☆☆☆☆☆

The following questions are targeted at digital service providers

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

○



Less than 10%

○ Between 10% and 50%

○ Over 50%

○ I cannot compute this information

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

	1 (not at all burdensome)	2	3 (neutral)	4	5 (very burdensome)	I don't know / No answer
Different processes and obligations imposed by Member States for notifying, detecting and removing illegal content/goods/services	○	○	○	○	○	○
Requirements to have a legal representative or an establishment in more than one Member State	○	○	○	○	○	○
Different procedures and points of contact for obligations to cooperate with authorities	○	○	○	○	○	○
Other types of legal requirements. Please specify below	○	○	○	○	○	○

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	○	○	●	○	○	○
Cooperation mechanism within Member States across different competent authorities responsible for the systematic supervision of online platforms and sectorial issues (e.g.						

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

3 Please explain

5000 character(s) maximum

Any regulatory/oversight body must be equipped with sufficient resources including financial and human, in order to be able to fulfil its mandate. The rag rug of poorly financed, understaffed data protection authorities in member states created by GDPR has shown that failing to enforce an otherwise well-done legislation can render crucial regulation toothless.

Cooperation schemes with civil society and academics can be useful but should not lead to an outsourcing of regulatory or oversight responsibility to non-governmental actors. The law must be enforced by the authorities, not by small non-profits struggling to scrape together funding to go to court against some of the largest and most powerful corporations in the world.

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

3000 character(s) maximum

At a minimum, competent authorities should publish:
(1) All their enforcement decisions such as decisions for remedies or sanctions/fines, including a comprehensive reasoning;
(2) Explanatory notes summarising each investigation for non-expert readers
(3) All raw data and supporting documents that were collected or analysed as part of investigations. These data and documents should be redacted to a minimum and only to protect the respective company’s IP and personal data.

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

Employees of competent authorities should have proven experience in the field of internet regulation, the platform economy and fundamental rights. They should never have any conflicts of interest with the companies they oversee. This is particularly necessary as big tech firms systemically coopt or co-finance the work of academics and other experts through grants—something that can potentially affect a person's independence.

6 In your view, is there a need to ensure similar supervision of digital services established outside of the EU that provide their services to EU users?

○ Yes, if they intermediate a certain volume of content, goods and services provided in the EU

○ Yes, if they have a significant number of users in the EU

○ No

○ Other

○ I don't know

7 Please explain

3000 character(s) maximum

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

3000 character(s) maximum

An EU regulator should have the ability to oversee service providers established outside of the EU regardless of their official company seat.

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

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

Coordinating the handling of cross-border cases, including jurisdiction matters	☆☆☆☆☆
Agreeing on guidance for consistent implementation of rules under the AVMSD	☆☆☆☆☆
Ensuring consistency in cross-border application of the rules on the promotion of European works	☆☆☆☆☆
Facilitating coordination in the area of disinformation	☆☆☆☆☆
Other areas of cooperation	☆☆☆☆☆

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

3000 character(s) maximum

14 Are there other points you would like to raise?

3000 character(s) maximum

Final remarks

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

1 Upload file

The maximum file size is 1 MB

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

8f505635-489b-45e3-b29c-934869ccd509/Panoptykon_DSA_consultation_submission_08.09.2020_final.pdf

2 Other final comments

3000 character(s) maximum

Useful links

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

Background Documents

(BG) Речник на термините

(CS) Glosř

(DA) Ordliste

(DE) Glossar

(EL) ά

(EN) Glossary

(ES) Glosario

(ET) Snastik

(FI) Sanasto

(FR) Glossaire

(HR) Pojmovnik

(HU) Glosszrium

(IT) Glossario

(LT) Žodynėlis

(LV) Glosārijs

(MT) Glossarju

(NL) Verklarende woordenlijst

(PL) Słowniczek

(PT) Glossrio

(RO) Glosar

(SK) Slovnk

(SL) Glosar

(SV) Ordlista

Contact

CNECT-consultation-DSA@ec.europa.eu