Contribution ID: 6a2d9039-29f2-4616-90f0-27788bdd760e
Date: 08/09/2020 19:50:00

Digital Services Act package: open public consultation

Fields marked with * are mandatory.

Introduction

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

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

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

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

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

Digital services and other terms used in the questionnaire

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

How to respond

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

Deadline for responses

8 September 2020.

Languages

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

About you

* 1 Language of my contribution

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

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

* 2 I am giving my contribution as

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

* 3 First name

Michael

* 4 Surname

TUNKS

* 5 Email (this won't be published)

mike@iwf.org.uk

* 7 Organisation name

255 character(s) maximum

Internet Watch Foundation (IWF)

* 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.

144739515066-23

* 21 Country of origin

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

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

12 What measure did you take?

- I reported it to the platform via its existing reporting procedure
- I contacted the online platform by other means to report the illegal content
- I contacted a national authority
- I contacted a consumer organisation
- I did not take any action

☑ I took a different action. Please specify in the text box below

13 Please specify

3000 character(s) maximum

The Internet Watch Foundation (IWF) receives reports from members of the public and is the only hotline in Europe that is currently permitted to proactively seek child sexual abuse online, thanks to a Memorandum of Understanding between IWF, National Police Chiefs' Council and the Crown Prosecution Service. Last year we discovered 132,700 webpages containing child sexual abuse imagery through a combination of reports from members of the public and our programme of proactive searching. We assessed 260,000 reports of suspected child sexual abuse imagery that had either been reported to us by the public or proactively found by our analysts.

In the first full year of proactive reporting (2014), the IWF actioned 118% more criminal imagery than the year before. Whilst we recognise the importance of providing the public with a safe place to report this abuse, there are challenges surrounding the accuracy of public reporting. In 2019, of the 110,000 reports received from the public, only 11% contained imagery confirmed to contain the sexual abuse of children. Off-remit reports are a waste of resources, resulting in illegal images staying live for longer, and raise serious concerns surrounding the welfare of our analysts when they view content that have not been trained to view.

We urge the European Commission to empower Hotlines across the Union to make use of their expertise. Providing Hotlines with an explicit legal role that standardises their powers, allowing them to view content, issue Notice and Takedowns, and proactively search for criminal content will ensure that these centres of expertise can be most effective.

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

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

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

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

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

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

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

- ◉ Yes
- ○ No

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

3000 character(s) maximum

Internet Usage has become a much bigger part of our daily lives as we all become much more socially distanced. Figures vary, but internet usage is said to have risen by 50% during covid-19 as the popularity of streaming services such as Netflix become even more popular with people spending more time indoors and at home. Children accessing educational material online, playing games and watching tv and films on multiple devices are also thought to be factors. Vodafone also reported that data usage was also up by 30%.

As a result of an increase in usage, Covid-19 has had a significant impact upon children and their protection online. The IWF has released several statistics which demonstrate the concerns we have about the protection of children now and into the future.

In the first month of lockdown, the IWF worked with three internet services providers and mobile network operators to measure the number of hits to the IWF's webpage blocking list. We found that a staggering 8.8 million attempts had been made to access known child sexual abuse material in the UK in just one month.

Between 23 March and 9 July, the IWF received 44,809 reports from members of the public. Compare that with 2019, when we received 29,698 and that represents a 50% increase, demonstrating that the public wants something done about these issues as well. Importantly, accuracy of public reporting remained at around its usual level. This meant that there was a 65% increase on the previous year's data in the number of webpages we actioned for removal as a result of public reports.

The threat to our children in their bedrooms continues to grow. In the first half of this year self-generated child sexual abuse content has increased representing 44% of all the imagery identified and removed by IWF. What's more, every day, IWF analysts deal with at least one instance of a child being groomed online to sexually abuse their younger sibling.

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

The IWF and other hotlines globally, have remained largely open for business and our organisation was designated as a “key worker” organisation during the pandemic by the UK Government, which enabled us to remain open processing public reports and proactively seeking content even through the national lockdown. We did go down to 50% capacity for a while but have reconfigured our office and we are now back to 100% capacity and have been since 1 June 2020. Staff that can work from home (not viewing content) are continuing to do so.

The IWF has been engaging with companies, Government, Law Enforcement and other NGOs throughout the pandemic to ensure that we are considering the potential threat to children during the lockdown. For example, the IWF has convened conversations with Government on how content is being moderated by companies during the lockdown and periods of working from home, ensuring that this content is being handled appropriately by the companies and still being swiftly removed.

The UK Safer Internet Centre has also been convening conversations with other charities during the pandemic through the UK Council for Internet Safety’s Early Warning Group to assist the UK Government in developing a picture of the threat to children during this period. We have also convened meetings with the internet industry to gain their feedback on the challenges they are facing. The UK’s National Policing Lead for Child Protection has also regularly been convening stakeholders and we regularly report into the law enforcement understanding of the challenge.

The IWF’s key services to industry, such as our URL blocking list, hash list and keywords lists have also remained operational and available to industry members throughout the pandemic uninterrupted which has also helped us minimise the availability of child sexual abuse material globally on the surface web.

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

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

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

3000 character(s) maximum

The IWF believes that more can and must be done to protect children online. We have responded to the Roadmap EU consultations on the Rights of the Child and the proposed EU strategy for a more effective fight against child sexual abuse, which in the main cover the steps we think must be taken to better protect children online. The EU has become the global hotspot for the hosting of child sexual abuse imagery and videos with the Netherlands in particular, responsible for 71% of the content we flagged for removal in the last year. We believe there should be a “child rights-based approach” with companies being asked to act within the best interests of the child and some way of holding companies to account over whether their systems and process are effective at doing this.

We have also called for a review of the current Child Sexual Exploitation Directive, in light of the fact that 23 Member States are facing legal action from the European Commission of non-conformities and the fact that issues such as grooming and live streaming in the online context are not covered by the current directive. We want to see a proposal for a Regulation from the European Commission, which compels Member States to take greater action.

The next step in the challenge for technology companies, who have collaborated effectively to help control the spread of child sexual abuse imagery and videos through the development of PhotoDNA and image hashing and through initiatives such as the Internet Watch Foundation and the US Tech coalition which have the ability to bring companies together to discuss new challenges in this area, is how we respond to the issues of grooming and live streaming, so far technical solutions to these challenges have evaded the companies.

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 IWF's role is distinct and we are experts in tackling child sexual abuse and exploitation online with the help and assistance of the European Commission, the UK Government, Technology industry and law enforcement. It is not appropriate for us to comment on areas which lie outside of our area of expertise. Our response to this consultation is distinct and limited to tackle child sexual abuse and exploitation online.

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

It is extremely rare for there to be erroneous removals for child sexual abuse images and videos. This is because there are clear laws defining what is child sexual abuse and there is broad international recognition that this imagery should not be circulating and be freely available online. In the UK we issue Notice and Takedown based on the guidance of the sentencing council guidelines (2014), which means that the same judgments of what is deemed to be illegal when a person is found in possession of these images, is the same judgment we reach when removing the content online. The expectations of the companies to remove this content is clear through the e-commerce directive, which states that companies should act "expeditiously" once they are notified that they are hosting illegal content. The hotline referral system ICCAM operated by INHOPE enables hotlines to transfer cases of CSAM to the appropriate country where the content is being hosted. This means it considers local laws and ensures that few mistakes are made in the removal of content.

In the UK, the Internet Watch Foundation's processes are open to scrutiny from an independent retired judge on a biannual basis. The retired former high court judge, currently Sir Mark Hedley, is responsible for reviewing and scrutinising our hotline operation and making suggestions for improvements to our operating procedures. Sir Mark also reviews areas of our work where the law is more open to interpretation. For example, the UK is the only place in the world where non-photographic indecent images of children (NPI) are illegal. There are different attitudes globally to this content and it is these challenges that we regularly consult with legal experts on.

Users have access to redress if they believe content that the IWF has actioned for removal is not child sexual abuse and they want it reinstated. The first step in this process is to appeal to us directly and the hotline manager and Deputy CEO and Chief Technical Officer will review the case in the first instance. If the complainant remains unsatisfied with the outcome of their initial appeal, then the complainant has the right to appeal through the Judicial Review process. Due to the nature of this content both appeals, and judicial reviews are extremely rare, certainly in the context of the UK environment.

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

The Internet Watch Foundation is recognised as the “appropriate authority” for issuing notice and takedown in the UK and we have a memorandum of understanding between ourselves, the National Police Chiefs’ Council and the Crown Prosecution Service that governs our operations. This grants our analysts immunity from prosecution for viewing child sexual abuse imagery, which is of course a criminal offence. The MoU also states that we have the authority to send “notice and takedown” to the internet industry in the UK. Thankfully, incidents of child sexual abuse are relatively small in the UK. Last year (2019) the IWF removed only 158 webpages in the UK that contained child sexual abuse material. This equated to less than 1% of the total number of webpages we flagged for removal internationally, with the Netherlands responsible 71% of the content and 89% of the content being hosted in Europe.

In the UK, removal of this content is extremely fast. 42% of content we asked companies to remove in the last year was removed in under two hours and the fastest recorded time from notice to removal is two minutes. It is important to recognise just how important the role industry play in removing child sexual abuse from their platforms, this is something that cannot be achieved without their co-operation. The IWF often finds it easier to remove content when we have a preexisting relationship with the industry member and they are fully paid up members of the IWF and are also implementing the range of technical services we offer to keep their platforms free of child sexual abuse in the first place.

In the case of US companies’, we will alert them about them hosting child sexual abuse content and alert the National Centre For Missing and Exploited Children (NCMEC) through a simultaneous alerts service in line with the companies obligation to mandatorily report content once they are notified of it on their servers.

Where the IWF particularly struggles is with its relationship with image hosting boards and cyberlockers. These hosts directly profit from hosting child sexual abuse, from known bad actors who frequently and rapidly migrate where they host this content to evade it being removed. 90% of the content the IWF actioned for removal were hosted on these types of services.

Because many of these services are hosted in the Netherlands (71% of all content we actioned for removal in 2019 was hosted there), they are also outside the jurisdiction of the IWF’s Notice and Takedown. We liaise with the in-country hotline and notify them, but resources for the volumes they are receiving are stretched and they are easily overwhelmed. After 48 hours pass the IWF can issue a direct notice to the responsible company for hosting the content, but removal times can vary and co-operation from some of those companies can take longer than if there was a pre-existing relationship, like the IWF has with many of its members.

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

3000 character(s) maximum

The IWF currently receives funding from the Connecting Europe Facility to provide 10% of our overall costs towards the operation of our hotline. This funding provides support for 50% of our analyst's salaries who are responsible for issuing Notice and Takedown and working internationally with other hotlines, our portal partners and in proactively searching globally for this content.

The overall operation of the Internet Watch Foundation for one year is £4million, but this includes the hotline operation, the development of world leading technology and services to the internet industry and data sets to keep their platforms free from child sexual abuse. It also means that we can carry out harm reduction activities through campaigns, public messaging and enables us to actively contribute to the policy landscape in the UK, EU and internationally by advising Governments on how best to deal with the issue of child sexual abuse imagery online.

It should be noted that industry already makes a significant contribution to the IWF on a voluntary basis, funding 90% of our activities.

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:

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

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

1000 character(s) maximum

The IWF annual reports provide a detailed breakdown of all the latest trends and data based our work and activities. These reports are published in April every year and are publicly available on our website on the following link:
https://www.iwf.org.uk/what-we-do/who-we-are/annual-reports

We also regularly release news and information through our media centre:
https://www.iwf.org.uk/news

And our responses to consultations in the EU, UK and Internationally can also be viewed here:
https://www.iwf.org.uk/what-we-do/who-we-are/consultations

In line with our grants process, we also provide the European Commission with information about the activities of the UK Safer Internet Centre.

Further information about our accounts, audits and inspections are available on the links below:
https://www.iwf.org.uk/what-we-do/who-we-are/accounts
https://www.iwf.org.uk/what-we-do/who-we-are/audits-and-inspections

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

9 Please indicate which one(s). What data is shared and for what purpose, and are there any constraints that limit these initiatives?

3000 character(s) maximum

Contractual obligations- The IWF provides data and information to online platforms, ISPs and other relevant actors in the internet ecosystem with the purpose of assisting platforms with keeping their services free from child sexual abuse and exploitation images and videos. This includes providing hashes, keywords, webpage blocking, simultaneous alerts, domain alerts, virtual currency alerts and payment brand alerts. Companies do share information when requested by the IWF, however, this tends to be on an informal and infrequent basis and has traditionally our requests have focused around measuring hits to our URL blocking list.

Data extraction approaches- The IWF is one of only three hotlines globally permitted to proactively seek out illegal child sexual abuse content and the only hotline in Europe permitted to carry out this function. The IWF' s web crawling technology enables us to gather large amounts of information much more quickly than a human analyst could. We use our human knowledge, skills and expertise to direct our web crawler using seed URLs and comparing the images it returns with our image hash list. It is important to note that web crawlers are not 100% accurate so there is still need for human review.

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

Our hotline analysts use several tools and services that are available from open source searches to find details and information about who may be responsible for the hosting of criminal imagery. This information is then used by our analysts to issue notice and takedowns, to remove this criminal imagery.

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

- (●) Yes
- ( ) No
- ( ) I don't know

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

3000 character(s) maximum

IWF analysts use WHOIS information to help them identify which hosting company is responsible for the public access to a website that has been found to contain criminal imagery, so that they can then issue a Notice-and-Takedown to the relevant company. WHOIS information is further used by our analysts to identify which Registrar controls the top-level domain, so that our analysts can advise the Registrar that a website under their ownership is hosting this imagery, and the website can be terminated.

One of the challenges with WHOIS, which has been well documented, is that its usefulness has been badly impacted, unintentionally, by the implications of the implementation of the EU's General Data Protection Regulation. The consequence of greater control over an individual's personal information and data, meant that ICANN reviewed the amount of publicly available data that was available through WHOIS and took the decision to remove the register as a source of open source data and it remains no longer freely available online. It is the IWF's understanding that relevant enforcement agencies such as law enforcement and hotlines are still able to access this data through requesting access to WHOIS information via ICANN and conversations are continuing within ICANN's Government Advisory Committee (GAC) about how to resolve the current impasse, however, progress remains glacially slow. The big implication for children, is that it now takes longer to identify a hosting company than it previously did. This is not something that can continue.

Our analysts and hotline team also when consulting the WHOIS database often find that it can contain erroneous and misleading information which is provided, unsurprisingly by people who have provided false details as a cover for their illegal activities (the dissemination of child sexual abuse material). It would be helpful in identifying who is responsible for these websites if more information was provided at registration through potentially the introduction of a "know your customer" principle.

13 How valuable is this information for you?

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

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

3000 character(s) maximum

The following questions are targeted at online intermediaries.

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

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

- [x] A notice-and-action system for users to report illegal activities
- [ ] 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
- [x] Automated systems for detecting illegal activities. Please specify the detection system and the type of illegal content it is used for
- [ ] Other systems. Please specify in the text box below
- [ ] No system in place

2 Please explain.

5000 character(s) maximum

The IWF, through a Memorandum of Understanding with the UK's National Police Chief Council and the Crown Prosecution Service, is recognized as the "appropriate authority" to issue Notice and Takedowns to companies hosting illegal images of children in the UK. Once our analysts determine that a URL fails UK law, a notice is issued to the company if it is UK based and it is removed by the hosting company. If we located content hosted outside the UK, the web page is added to our URL blocking list until such a time as it is removed by the company, at which point the URL is removed from our blocking list. The IWF response has been instrumental in the UK zero-tolerance approach to the hosting of this content and has been instrumental in reducing UK hosting of globally known content from 18% in 1996 to just 0.1% in 2019. The UK has consistently hosted less than 1% of globally known content since 2003.

The IWF offers a range of unique, preventative services to industry Members to prevent this abuse from being available on their platforms or services. In addition, the IWF is currently developing a range of automated services (image classifiers and web crawlers) to supplement the work of our analysts. However, we believe that it is critically important that human moderators remain central to any response as currently there is no technology that can accurately assess the age of a child. This becomes particularly difficult as the child goes through puberty. For example, it becomes particularly difficult to accurately assess the age difference between a 17 or 18-year-old. Some adult performers also look like they could be younger than 18, which without the insight of our analysts having reviewed that content regularly previously, may reach the wrong conclusion and remove content which is legal. Our analysts are expertly trained to make these difficult judgements, and any new content actioned by the IWF is checked by human eyes, so we can be sure that we are only removing illegal content. Relying heavily on technical solutions heightens the risk of false positives, undermining the efforts of all actors working to eradicate this content and increasing the pressure in the court process with higher volumes of judicial reviews.

Our bespoke, highly intelligent crawlers support the work of our analysts by crawling through millions of webpages, identifying known images of child sexual abuse. We train our crawler by feeding it with URLs that we know contain CSAM and then check any matches against our image hash list. This allows us to more quickly identify potential incidents of suspected CSAM and allows our analysts to focus their efforts on identifying new content, whilst providing victims with the closure that their images are being removed from the open web.

3 What issues have you encountered in operating these systems?

5000 character(s) maximum

The most effective way of addressing illegal content is to remove it at source. However, the legal systems within some European Member States hinder the effectiveness of this response. For several years, the IWF has seen a steady rise in the hosting of illegal content in Europe, specifically the Netherlands. In 2019, the IWF assessed 132,000 webpages confirmed to contain the sexual abuse of children. Of these 89% were hosted within Europe, and 71%, or 94,000 URLs, were hosted in the Netherlands. There was first a shift in the hosting of this content in the Netherlands in 2016, when our annual report highlighted an 18% increase on the previous year, and this is a trend that has continued in the years since. This illegal content will always be hosted in areas where it remains live for longest and where it is most difficult for it to be removed.

The legal infrastructure of the Netherlands makes it difficult to effectively address this crisis. Several of these 'bulletproof-hosters' are unwilling to co-operate with hotline requests to remove content and state they require a court order to remove the illegal content. This is in direct contravention of the e-commerce directive, where they are supposed to act expeditiously and pursuing each of the 94,000 URLs the IWF identified in Dutch hosting space in 2019 would overwhelm the courts. Indeed it is already overwhelming the Dutch hotline, who reported in their annual report that they were dealing with a backlog of cases. In the UK, the IWF is empowered to act before the court process, and claimants can appeal any decision made by the IWF through the court process if they believe the decision to be incorrect. This approach allows the imagery to be removed swiftly and effectively, whilst providing a clear avenue for appeal. Our processes are also compliant with Human Rights and are subject to regular bi-annual review from a High Court Judge, which further gives confidence to companies, law enforcement, Government and the Courts that we are acting appropriately when issuing notice and takedown.

Further technical and legal challenges for the IWF is that at present we are unable to pass through paywalls, or enter encrypted channels, such as private messaging platforms. As there is a greater move towards introducing encryption across services, this poses a real challenge to the mission of the IWF, as the ability of industry to screen for known criminal content, and for law enforcement to collect evidence of criminal activity is greatly reduced as neither the companies, nor law enforcement will actually be able to see what is being sent over an encrypted channel and the only way of them becoming aware of this would be for the end user to notify them of what they have been sent.

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

In 2019, the IWF assessed 260,426 reports of suspected child sexual abuse imagery. These reports primarily came from the IWF proactive searching (56%) and public reporting (41%). Of these, 132,676 URLS were confirmed to contain the sexual abuse of children – each webpage could contain anything from one to thousands of images, equating to millions of images removed by our analysts.

The IWF's remit is distinct and limited to images and videos of child sexual abuse, and our analysts assess in line with UK law. In 2019, 20% was assessed to be Category A, 20% Category B, and 58% Category C. A full breakdown of UK law and assessment levels in this space can be found here.

A full breakdown of IWF's 2019 figures can be found here. The full catalogue of our recently published annual reports can be found on our website.

No official appeals made against the IWF's moderating decisions have been upheld, and therefore no content has been reinstated. Since 2014, the IWF has recorded 167 complaints have been made to the organisation, however these have not all been in relation to specific moderation decisions made by the IWF, or even related to our work. For example, we receive complaints when users have been wrongly informed that we are responsible for their difficulty connecting to a website. In 2019, we received 41 complaints regarding URLs that had been placed on our block list and 3 complaints regarding a notice and takedown decision. None of these complaints were upheld.

Every two years, the IWF is independently audited by a small team of experts, led by Sir Mark Hedley, a high court judge, to monitor our decision making and ensure the standard of our work. In their most recent inspection, the team was 'satisfied that reasonable judgements to consistent standard were being made' and that this was 'kept under proper review'. The full report can be found on our website.

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

Any site, owner of a company, or individual can appeal against a decision made by the IWF if they believe that the webpage did not originally contain criminal imagery. The IWF then reviews this decision internally, to determine whether a mistake or error was made by our analysts. The IWF has never upheld an appeal that has been made. From the 1 January 2018 to 3 October 2019, the IWF received 54 complaints regarding the blocking of a website. Examples of each complaint were reviewed and not upheld either because evidence had been captured showing that the URL had been hosting illegal content, or because the extent of the website access to the site which had been blocked by the ISP had been in excess of that requested by the IWF.

Once having internally reviewed the appeal, the IWF reports back to the claimant. If they so wish, the case can be passed to law enforcement for review and get their assessment. If law enforcement agrees with the assessment of the IWF, and claimant wishes to continue to pursue an appeal, then ultimately, they can request Judicial Review. However, in 24 years of operation, this has never happened.

A full break down of the IWF appeal process can be found here. If the IWF were to review a case and determine that there had been an error on behalf of the organisation, the URL would be removed from the URL block list or the Notice and Takedown repealed.

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

Whilst the IWF does utilise automated services to support the work of analysts, we firmly believe that human moderators must remain at the centre of assessment process. There is no technology that can accurately age a child, and we ensure that our expert, human analysts, lead the assessing and actioning of our reports. It is notoriously difficult to judge the age of a child once they have reached puberty, and if analysts identify a victim who they believe to be over 14 they are required to seek a second opinion. The IWF has an inbuilt quality assurance function, and our quality assurance team perform regular dip-tests to ensure consistency in decision making across the Hotline.

Our bespoke, highly intelligent crawlers support the work of our analysts by crawling through millions of webpages every day, identifying known images of child sexual abuse against our hash list. This crawler does not identify new images of abuse, though can provide analysts with intelligence that they can then pursue.

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

- [x] Yes
- [ ] No

5 Please explain.

5000 character(s) maximum

Governed by a Memorandum of Understanding between the National Police Chiefs' Council and the Crown Prosecution Service, the work of the IWF is rooted in a robust legal basis. We assess imagery and videos in line with the Sentencing Council Guidelines (2014) which categorises illegal child sexual abuse content into Category A, B, C and not illegal. As such, our work must remain in line with UK law standards, where the same judgment reached in convicting offenders of possessing these images is the same that is reached when our analysts request removal by issuing notice and takedown. Our work is regularly reviewed through a biannual Hotline audit overseen by Sir Mark Hedley, a high court judge. In these audits, the inspection team reviews the training of our analysts, the consistency and standard of our work, and our reviewal and evaluation processes for monitoring our work. The IWF is also an ISO 270001 accredited organisation.

As discussed above, any claimant wishing to appeal a decision made by the IWF can refer our assessment to law enforcement and, in the final case, to Judicial Review.

D. Transparency and cooperation

1 Do you actively provide the following information:

- [x] Information to users when their good or content is removed, blocked or demoted
- [x] 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

Full details of the IWF's work removing CSAM can be found in our annual reports.

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

It would be inappropriate for the IWF to fully explain the process our analysts go through when removing child sexual abuse material as it could inadvertently direct people to proactively seek out known child sexual abuse imagery. However, we are committed to being as transparent as we possibly can be and details of how we assess and remove content can be found on our website.

Automated tools which assist our analysts with the identification of illegal content are still largely in the development phase. The IWF gave some information to the Independent Inquiry into Child Sexual Abuse's Internet Inquiry on how the web crawlers function and we ensure that any information the crawlers process is in complete compliance with the European Union's General Data Protection on the processing of personal data. Our image classifiers are still in development and not in full operational use.

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

- [x] Contractual conditions
- [x] Special partnerships
- [ ] Available APIs (application programming interfaces) for data access
- [x] Reported, aggregated information through reports
- [ ] Portability at the request of users towards a different service
- [x] 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 IWF exists as part of a trusted partnership between industry, Government, and Law Enforcement, and shares data with each to eradicate the imagery of child sexual abuse online most effectively. We share data with relevant Government departments and Law Enforcement agencies to inform these stakeholders on the nature and scale of the threat we are facing, on changing offender practices and trends, and to safeguard users. We are the only non-governmental organisation connected to the UK's Child Abuse Image Database, and able to feed in our own hashes and images of criminal content to complement law enforcement's database of forensic captures. We are also a trusted voter, one of three votes needed that helps law enforcement to categorise hashes already within the database so they can be used in court processes. The IWF also shares its hashes with industry directly and indirectly by inputting our hashes into the NGO sharing platform hosted by the National Centre for Missing and Exploited Children, this allows us to pool our hashes and ensuring that industry can proactively prevent more content from being uploaded.

The IWF shares its data sets directly with industry Members to allow companies to proactively prevent child sexual abuse from being disseminated on their networks, services, or platforms. These data sets are only available to Members who have passed the IWF's internal due diligence processes and entered into a contractual agreement with the IWF that outlines the specific circumstances in which these data sets can be used.

The IWF is regularly audited to ensure compliance with all relevant data protection laws. Further information on the auditing process can be found here.

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

The IWF believes that it is extremely important that industry cooperates effectively in the removal of illegal child sexual abuse imagery and material. Many of the companies within the IWF membership do so on a voluntary basis by paying into the IWF and committing to do all that they can by taking our services that assist them in keeping their platforms free of this abhorrent imagery. As we have referenced elsewhere in our response, the challenges are with those companies who don’t wish to join the IWF and fail to act without a court order. We strongly believe that “trusted flaggers” play an important role in the online environment and if there was a legal obligation that compelled image hosting boards and cyberlockers to comply with orders from hotlines, this could go some way to eradicating the current situation in Europe. We also believe that if they were to deploy IWF services in the first place, much of this material could be prevented from circulating.

On the issue of content moderation, in an ideal world, companies would of course have moderation teams to deal with illegal content, however, we need to consider carefully the implications and regulatory burdens that we place on businesses. It is simply not conceivable for small start-ups to employ content moderators. We believe that the EU needs to focus on creating a regulatory environment that ascertains how companies detect and remove illegal or harmful content and audits companies on how they are complying with the legal framework. This is something which is currently being given careful thought to through the UK’s Online Harms legislation and many of the same arguments rehearsed in the development of that legislation could also be applied to the European Commission’s proposals for a Digital Services Act.

We haven’t commented on areas that sit outside of the IWF’s remit in tackling child sexual abuse in the above section.

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

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

4 Please explain

3000 character(s) maximum

The more information that a user can provide, the quicker and easier it is to assess the content and, if illegal, work to have it removed. To facilitate ease of reporting, it would benefit the user if these reporting processes were standardised across platforms, and if a consistent approach to the information requirements was taken.

Users should have the option to provide their details if they wish to receive a response to their complaint, but this should not be a requirement of the reporting process. This is because many reporters fear reprisal from law enforcement for reporting criminal content. Around 80% of reports the IWF receives are reported anonymously. Our independence from law enforcement is helpful in encouraging people to report. Such a requirement could introduce friction into the reporting process, disincentivises users from coming forward, and ultimately undermine the benefit of reporting processes - users are often anxious of the potential consequences surrounding identifying illegal content.

The IWF provides users a with a secure, confidential, and anonymous place to report suspected child sexual abuse imagery. Though reporters can provide details if they so wish, our system is designed to instill confidence and security.

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

Illegal Child Sexual Abuse Imagery and Videos that have been previously identified by the IWF should not be reappearing online. Once an image is hashed, provided companies are deploying the IWF hash list it should be prevented from being reuploaded online, if companies are properly deploying the IWF hash list and scanning against uploaded images for potential matches of illegal content we have previously identified. We also know that Internet Service Providers and other internet companies can utilise our URL blocking list, whilst we are removing that content at source, which can also stop countless eyes from viewing child sexual abuse in the meantime. Search Engines can also optimise their searches by using our keywords list to prevent the return of illegal CSAM. With new imagery, it is of course much harder to detect initially for companies. Technology such as image classifiers can of course assist in detecting skin tone, but as we have mentioned elsewhere in this consultation, it cannot be relied upon to accurately detect imagery that is not previously been detected, as there is a high probability that this imagery could be removed inaccurately.

There are emerging challenges around grooming and live streaming, to which yet there are not technical solutions to prevent these things from occurring online. We would like to see the European Commission continuing to invest in education and awareness raising initiatives to warn children and young people, parents and those who educate them about these dangers online. We also want the European Commission to take an approach that is in the best interests of the child by incentivising companies to work together to tackle these incredibly complex challenges and achieve the best possible outcomes for children.

We believe that companies should be compelled to put in place relevant tools and services that help to protect their users as part of a duty of care. However, it is important that proportionately is not undermined in the process. We believe that tech companies could take advantages of services from organisations like the Internet Watch Foundation to keep their platforms free from child sexual abuse. We do, however, believe that the European Commission needs to be careful about prescribing technological solutions to these challenges in primary legislation. We want to see primary legislation that is principle based, clearly sets out obligations and expectations of companies and secondary legislation through codes of practice that then provide guidance and clarity on how the companies are expected to demonstrate their compliance with the new regulatory requirements. Legislation will never be able to keep pace with technological developments and therefore it is important that the Commission isn’t continually having to change primary legislation because technology has moved on.

We also believe that Member State legislation needs to be addressed if we are to be successful in ridding Europe from the scourge of child sexual abuse. We have made a number of recommendations that need to be taken in our response to the Roadmap on a more effective fight against child sexual abuse.

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

3000 character(s) maximum

The IWF provides its Members with a range of tools allowing industry to proactively and preventatively screen for illegal content. All the services provided by the IWF are quality assured by our in-house team, so that industry Members can be confident that any material blocked or identified does comply with UK and EU legal frameworks. These services allow industry to prevent users from accessing this criminal content; if they were to try and access a site blocked by our URL list, they are instead returned a splash page outlining why this content has been blocked, and signposting to further support. Our hash list allows companies to proactively prevent known imagery from being further disseminated on platforms, protecting the victim from further revictimisation, and our keywords list allows companies to filter results on search engines and present abusive imagery from being returned. All these tools allow content moderators and analysts to focus their efforts elsewhere, identifying 'new' or even recent imagery, and safeguards both users and victims. These automated processes also make it harder for internet users to stumble across this content and, perhaps inadvertently, commit an offence.

The IWF can provide these services with these assurances due to the distinct, clear legal basis that we work in – what constitutes criminal imagery of children is clearly set out in UK law. This is not quite so clear in relation to other harms, or areas. Focusing on the remit of the IWF, there are currently no technical solutions to identify the livestreaming of abuse or identify grooming, and challenges exist around rapidly responding to this abuse, and accounting for context. Further implementation of automation into areas that lack this clear legal basis risks the rise of false positives and false negatives, undermining public faith in these processes, the moderators, and the platforms that deploy them.

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

Child sexual abuse material online is a global issue, that transcends the traditional boundaries of both national and supra-national legislation and jurisdictions. It is often the case that an offender could be watching abuse from one country, with the child being abused in a second, that is hosted or facilitated by a platform in a third. The other challenge is that often this content can be taken down and rapidly migrated to a new hosting country, before the whole process starts again. To address the scale of the challenge, it is critical that the European Commission adopts a collaborative and cooperative approach and commits to safeguarding its users in this increasingly interconnected world.

When implementing new legislation, the European Commission must take great care in ensuring that any changes complement the current existing measures being taken elsewhere in the world. The Commission has announced new plans for a Centre to tackle child sexual abuse and exploitation which is welcomed, but if it introduces mandatory reporting obligations on European companies or those offering services to European citizens, then it must be careful not duplicate effort by starting investigations, which may already have been started in the US due to its mandatory reporting laws. We would urge the European Commission to have early conversations with the five eye countries (UK, NZ, Aus, Canada, US) about the approach they are taking to these issues and seek to complement that approach in any EU legislation. The five eye's voluntary principles are a good starting point for requiring further action by technology companies on a voluntary basis.

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

We strongly believe that the European Commission has an excellent opportunity to address the appalling hosting problems of child sexual abuse imagery in the Netherlands and the EU as a result of the Digital Services Act. We want to see image hosting boards and cyberlockers brought within the scope of this legislation and we certainly believe that they could be doing much more to tackle illegal content and the illegal use of their services. They are responsible for 90% of the child sexual abuse images and videos that the IWF acted upon in the last year. In many instances it is a combination of weak national legislation that enables the companies to take advantage of the situation, however, we believe that many of these companies responsible for this content know who the individuals are responsible for the spread of CSAM and more could be achieved through a know your customer principle, which would prevent offenders from quickly being able to regularly migrate their domains to new countries to avoid detection. The biggest challenge is getting the “bad actors” who refuse to co-operate with hotlines, law enforcement around the table to discuss the challenges that they create. Those who join the IWF are genuinely trying to do the right thing and are an active part of the conversation. Their membership fees often pay to help clean up the mess left behind by bad actors, which is neither right nor fair.

The IWF’s Membership currently includes several of these online intermediaries and we provide a range of services to them that are suitable for their business models. Internet Service Providers, for example, take and deploy our URL blocking list, to prevent users from accessing this criminal material. All digital services can play a role in eradicating this abusive imagery. The IWF’s membership also includes providers of DNS Services and we provide Domain Alerts, which help them to build a picture on how their services might be being abused. Whilst the ability to act is diminished the lower down the internet stack you go, we do believe that everyone has their part to play and the broader the scope of any regulation on Digital Services, the more opportunity you have for everyone to play their part. The expectations of the various actors in the different layers of the internet ecosystem can then be addressed through guidance or if necessary secondary legislation.

In designing this new regulatory environment, the European Commission must continue to work with organisations that have a deep technical understanding of the global internet landscape. The IWF has significant experience of working with all types of companies across the internet ecosystem and looks forward to continuing to work with the European Commission to eradicate this abuse.

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

- The IWF believes that there is no place for imagery depicting the sexual abuse of children on the internet today.

- Industry should be encouraged to take all relevant services that can prevent the upload and dissemination of this abuse and engage in regular transparency reporting that is defined by clear metrics.

- The Commission should consider the appointment of trusted flaggers in identifying this content and working with industry to have it removed.

However, the European Commission must uphold the delicate balance between protecting children from harm, whilst ensuring their right to freedom of expression, privacy, education, and play. The internet is a force for good and provides children with a wealth of opportunities to learn, socialise, and engage in civic and political discussion. These fundamental rights must be respected as we work to eradicate abuse from these platforms; children cannot have their online experience limited or removed in response.

Safety by design should be at the very heart of the development process, and the IWF would point the Commission towards the UK's Age Appropriate Design Code as an example of best practice in this area. The Code centres the best interests of the child and outlines 15 principles for industry to follow to ensure that their services are suitable for children. This approach cements children's right to engage in the online environment, whilst ensuring that industry providers are safeguarding them from potential risks.

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

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

5000 character(s) maximum

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

	1 (not at all necessary)	2	3 (neutral)	4	5 (essential)	I don't know / No answer

Transparently inform consumers about political advertising and sponsored content, in particular during election periods	○	○	○	○	○	◉
Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with user complaints	○	○	○	○	○	◉
Tackle the use of fake-accounts, fake engagements, bots and inauthentic users behaviour aimed at amplifying false or misleading narratives	○	○	○	○	○	◉
Transparency tools and secure access to platform data for trusted researchers in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it	○	○	○	○	○	◉
Transparency tools and secure access to platform data for authorities in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it	○	○	○	○	○	◉
Adapted risk assessments and mitigation strategies undertaken by online platforms	○	○	○	○	○	◉
Ensure effective access and visibility of a variety of authentic and professional journalistic sources	○	○	○	○	○	◉
Auditing systems for platform actions and risk assessments	○	○	○	○	○	◉
Regulatory oversight and auditing competence over platforms' actions and risk assessments, including on sufficient resources and staff, and responsible examination of metrics and capacities related to fake accounts and their impact on the manipulation and amplification of disinformation.	○	○	○	○	○	◉
Other (please specify)	○	○	○	○	○	◉

13 Please specify

3000 character(s) maximum

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

3000 character(s) maximum

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

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

16 Please explain.

3000 character(s) maximum

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

- Transparency is key, and companies should be required to release information to relevant authorities, to set metrics, on the content that they flag, assess, remove, and, if relevant, reinstate following appeal. This information should also be broken down in how it was identified – be it through reports from users, content moderators, or through automation.
- Currently, the transparency reporting undertaken by industry is patchwork at best. Many companies are currently releasing information based off metrics that they have devised in-house, the categories of which differ. This makes it difficult for Government, law enforcement, or relevant stakeholders to gauge the size of the threat.
- This patchwork approach also means that the fraction of industry members who are currently engaging in this reporting are likely to be penalised for this transparency. Such consequences are not the result of these companies being guilty of the worst abuse, but of being willing to discuss the problem.
- However, the Commission must consider the usefulness of compelling industry to release numbers without any context. Such a practice highlights the danger of creating panic, forcing actions that do not address the problem that we are facing. Similarly, there are risks surrounding the release of information to the public, as opposed to designated expert organisations who understand the complexity of the issue at hand, and able to usefully place this data in context and apply it to a long-term, impactful, response.
- We do not believe, however, that it would be appropriate for industry to release content outlining the specifics of the content they have removed or blocked, or where this content was blocked from. The IWF URL blocking list can, on average, contain anything from 6,000 – 12,000 URLs everyday containing imagery of children being sexually abused. We are exceptionally careful to ensure that this information remains private, and similarly we do not name and shame guilty sites, as doing so might inadvertently drive more traffic towards this images, and ultimately revictimise the children who suffered this abuse.

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

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
- [x] 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
- [x] Specific request of law enforcement authority or the judiciary
- [ ] On a voluntary and/or contractual basis in the public interest or for other purposes

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

5000 character(s) maximum

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

5000 character(s) maximum

24 Are there other points you would like to raise?

3000 character(s) maximum

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

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

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

For two decades, the e-Commerce Directive has fundamentally set the parameters for industry to thrive whilst removing illegal content from their platforms, precisely due to its clarity. The IWF believes that this is an essential piece of legislation and urges the European Commission to ensure that any revisal to the liability regime retains this clarity of scope. We would encourage the European Commission to maintain the e-Commerce Directive's focus on content that is clearly defined as illegal, rather than broadening into the arena of legal but harmful. Attempts to moderate these areas, without clear guidelines, leads to inconsistency in decisions from moderators, results in the over-removal of content, and undermines consumer trust in the digital economy.

However, the current liability regime outlined in the e-Commerce Directive faces challenges as more companies move towards the adoption of end-to-end encryption. When written, the e-Commerce Directive allowed industry to thrive through accepting that the sheer amount of user generated content uploaded every second makes it impossible to moderate each piece. But now, questions must be raised about how this liability regime affects organisations making themselves blind to content on their platforms, being unable to moderate interactions between users, and, inadvertently, creating safe spaces for the dissemination of this abuse. There is a difference between being unaware of illegal content and being intentionally blind to said abuse.

The e-Commerce Directive, as it currently stands, faces further challenges against this increasingly internationally crisis. The problem of child sexual abuse imagery transcends traditional borders and requires an international response, reaching beyond the borders of the European Union. The territorial scope of the current Directive limits the impact that it can have to protect children, and European users, across the globe. Therefore, the IWF supports the proposal laid out in Option 2 of the 'Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services' to extend coverage of such measures to all services directed towards the European single market, including when established outside the Union.

4 Does the current legal framework dis-incentivize service providers to take proactive measures against illegal activities? If yes, please provide your view on how disincentives could be corrected.

5000 character(s) maximum

The IWF has worked closely with the internet industry for the last 24 years, and consistently found that many of industry's leading players have been keen to proactively address the potential for the exploitation of children on their platforms. The fact that these major competitors often regularly convene and converse in conversations about how to tackle CSEA through the IWF funding council and regularly share their engineering expertise, insights, tools and developments with each other through the IWF is remarkable and a very unique thing that should be treasured and safeguarded. The current legal framework through the DSA incentivises companies to remove child sexual abuse content once they are made aware and many have invested significant time and energy in to developing technology such as photo DNA to assist in that fight.

However, companies are currently limited on taking more proactive steps themselves. If their engineers were to proactively seek child sexual abuse on their networks, this action is, in and of itself is a criminal offence. Article 15 of the e-commerce directive, currently prevents companies EU Member States from imposing on intermediaries a general obligation to monitor information which they transmit or store and provides that intermediaries cannot generally be obliged "actively to seek facts or circumstances indicating illegal activity."

Despite the very complex nature of encouraging technology companies to take a much more proactive approach there are significant challenges in altering Article 15. When the House of Lords Communications Select Committee investigated this exact issue in its report: "Regulating in a Digital World" , it referenced competing evidence from different quarters. It heard evidence from the Children's Media Foundation and the Northumbria Internet and Society Research Interest Group, which called for reform of the Article, stating it was twenty years old and in need of reform.

However, others such as Oath and Global Partners Digital stressed the importance of cautioning against "inappropriate legislation" which could have a "chilling effect" and could place too much power in the hands of technology companies to make decisions about what is and isn't illegal, leading potentially to an over-removal of perfectly legal content, because ultimately these tech companies are not best placed to make these decisions. Global Partners Digital went on to say that the minimal transparency, absence of due process, safeguards for affected users and oversight would also exacerbate the problems faced. This a view that the Internet Watch Foundation also shares.

Eventually, however, the House of Lords Committee concluded that online platforms have developed new services which were not envisaged when the e-commerce directive was introduced. They now play a key role in curating content for users and going beyond their role as a simple hosting platform.

The Internet Watch Foundation would welcome more proactive steps from companies, however, they would need to be carefully guided, helped and supported by those organisations who have understanding, expert knowledge and expertise in making assessments and judgements about what does and does not constitute illegal activity and this work would have to be properly and appropriately resourced.

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

The IWF recognises that it is not feasible or proportionate for industry players to be legally responsible for every piece of content that is uploaded to their networks. However, the recent move towards greater encryption has presented serious challenges to the prevention of the dissemination of known child sexual abuse material. The concept outlined above does not take into consideration the role of service providers in crafting the online environments that so much of our lives exist in. Decisions regarding the development and deployment of services defines how users interact with them, and how law enforcement can operate within them. Any update to the e-Commerce Directive should highlight the role these service providers play, and place responsibility on the decisions taken when developing and implementing services, including a full risk-assessment. For example, the DNS over HTTPS standard, recently adopted by the Internet Engineering Task Force, had the potential to inadvertently undermine blocking lists for both child sexual abuse material and terrorist content, as the policy focus was not matched up to the technical development.

Similarly, the move towards end-to-end encryption on messaging services raises serious concerns around the ability of industry to undertake preventative, and monitoring measures, and risk these platforms becoming ‘safe havens’ for this abuse. The IWF encourages the Commission to consider proposals surrounding companies to consider safety-by-design at the very start of the development process, and to identify any inadvertent risks to users and to the dissemination of child sexual abuse material.

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

When crafting the Digital Services Act, the European Commission must uphold the delicate balance between protecting users' rights to privacy with the rights of children to a secure childhood, free from sexual abuse and exploitation. The right to privacy of the victim of this abuse, too, cannot be overlooked. Any new legislation should also consider and complement the European Commission's General Data Protection Legislation. The ongoing debate surrounding the e-Privacy legislation has highlighted many of the challenges in this space, as the Commission has sought to balance user rights and tackle the issue of child sexual abuse. The same mistakes that have bound the e-privacy file up in amendments and delay for the past three years must be avoided in the development of the Digital Services Act.

This is an extremely difficult area to legislate in. The European Commission must pay careful attention to the UN declaration on Human Rights Article 12, which declares an individual's right to freedom from interference with their privacy, family, home or correspondence. These rights have been hard fought for and many of the EU Member States are signatories to the Declaration on Human Rights.

We should, however, make clear that whilst the right to privacy is a fundamental right, it is not an absolute right and that right can be controlled and are subject to reasonable restrictions for the protection of general welfare, something which of course, is absolutely at the heart of tackling the spread of child sexual abuse online.

When considering the introduction of general monitoring obligations, the European Commission must carefully consider the impact that such requirements will have on all industry, not just the largest tech companies. The scale of the challenge we face should not be underestimated, and nor should the potential burden on small and medium sized enterprises. The European Commission must be careful not to stifle innovation, through creating a regulatory environment that prevents smaller companies or new services from thriving in this competitive, fast-moving market. Recent global events have highlighted how rapidly services can grow; as schools and offices were forced to close throughout Europe, video-conferencing platforms surged in demand, with Zoom alone reporting a 30-fold increase in April. The requirement for general monitoring obligations becomes increasingly difficult when platforms unexpectedly see such a surge in users without the infrastructure to support them.

The IWF recommends that the European Commission carefully considers and further consults on this area taking into account the views of the technology industry, hotlines, law enforcement, before seeking to establish exactly what the requirements may be for general monitoring and what the expectations could be of such an obligation and what the potential consequences of implementing such an approach may be.

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

The IWF supports many of the proposals the European Commission laid out in Option 2 of its recent roadmap on the 'Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services'. We are particularly supportive of the suggestion of harmonising a set of specific, binding and proportionate obligations that outline the different responsibilities for online platforms and believe that the current liability regime could be improved through the provision of a specific, legal role of Hotlines. Empowering Hotlines throughout Europe to issue notice and takedowns would make best use of these centres of expertise and experience, and would lighten the load on law-enforcement agencies – allowing them to focus their limited resources on safeguarding victims, identifying and arresting offenders and dismantling commercial gangs. These recommendations have been further outlined in the recommendations made by the European Parliament's LIBE Committee in November 2017.

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

10 In your view, what practices related to the use and sharing of data in the platforms' environment are raising particular challenges?

5000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

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

3000 character(s) maximum

Regulation of large online platform companies acting as gatekeepers

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

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

2 Please explain

3000 character(s) maximum

3 Do you believe that such dedicated rules should prohibit certain practices by large online platform companies with gatekeeper role that are considered particularly harmful for users and consumers of these large online platforms?

- Yes
- No
- I don't know

4 Please explain your reply and, if possible, detail the types of prohibitions that should in your view be part of the regulatory toolbox.

3000 character(s) maximum

5 Do you believe that such dedicated rules should include obligations on large online platform companies with gatekeeper role?

- Yes
- No
- I don't know

6 Please explain your reply and, if possible, detail the types of obligations that should in your view be part of the regulatory toolbox.

3000 character(s) maximum

7 If you consider that there is a need for such dedicated rules setting prohibitions and obligations, as those referred to in your replies to questions 3 and 5 above, do you think there is a need for a specific regulatory authority to enforce these rules?

- Yes
- No
- I don't know

8 Please explain your reply.

3000 character(s) maximum

9 Do you believe that such dedicated rules should enable regulatory intervention against specific large online platform companies, when necessary, with a case by case adapted remedies?

- Yes
- No
- I don't know

10 If yes, please explain your reply and, if possible, detail the types of case by case remedies.

3000 character(s) maximum

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

- Yes
- No

12 Please explain your reply

3000 character(s) maximum

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

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

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

3000 character(s) maximum

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

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

High level of technical capabilities including data processing, auditing capacities

- [ ] Cooperation with extra-EU jurisdictions
- [ ] Other

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

3000 character(s) maximum

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

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

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

3000 character(s) maximum

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

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

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

3000 character(s) maximum

27 Are there other points you would like to raise?

3000 character(s) maximum

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

Online advertising has substantially evolved over the recent years and represents a major revenue source for many digital services, as well as other businesses present online, and opens unprecedented opportunities for content creators, publishers, etc. To a large extent, maximising revenue streams and optimising online advertising are major business incentives for the business users of the online platforms and for shaping the data policy of the platforms. At the same time, revenues from online advertising as well as increased visibility and audience reach are also a major incentive for potentially harmful intentions, e.g. in online disinformation campaigns.
Another emerging issue is linked to the conclusion of 'smart contracts' which represent an important innovation for digital and other services, but face some legal uncertainties.
This section of the open public consultation seeks to collect data, information on current practices, and informed views on potential issues emerging in the area of online advertising and smart contracts. Respondents are invited to reflect on other areas where further measures may be needed to facilitate innovation in the single market. This module does not address privacy and data protection concerns; all aspects related to data sharing and data collection are to be afforded the highest standard of personal data protection.

Online advertising

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

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

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

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

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

3000 character(s) maximum

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

3000 character(s) maximum

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

Please rate your level of satisfaction	☆ ☆ ☆ ☆ ☆

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

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

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

3000 character(s) maximum

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

Please rate your level of satisfaction	☆ ☆ ☆ ☆ ☆

The following questions are targeted specifically at online platforms.

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

3000 character(s) maximum

11 Do you publish or share with researchers, authorities or other third parties detailed data on ads published, their sponsors and viewership rates? Please explain.

3000 character(s) maximum

12 What systems do you have in place for detecting illicit offerings in the ads you intermediate?

3000 character(s) maximum

The following questions are open to all respondents.

14 Based on your experience, what actions and good practices can tackle the placement of ads next to illegal content or goods, and/or on websites that disseminate such illegal content or goods, and to remove such illegal content or goods when detected?

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

Smart contracts

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

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

2 Please explain the difficulties you perceive.

3000 character(s) maximum

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

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

3000 character(s) maximum

5 What capabilities – type of internal expertise, resources etc. - are needed within competent authorities, in order to effectively supervise online platforms?

3000 character(s) maximum

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

- Yes, if they intermediate a certain volume of content, goods and services provided in the EU
- Yes, if they have a significant number of users in the EU
- No
-

Other

I don’t know

7 Please explain

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

3000 character(s) maximum

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

rules?

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

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

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

3000 character(s) maximum

14 Are there other points you would like to raise?

3000 character(s) maximum

Final remarks

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

1 Upload file

The maximum file size is 1 MB
Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

2 Other final comments

3000 character(s) maximum

Useful links

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

Background Documents

(BG) Речник на термините

(CS) Glosř

(DA) Ordliste

(DE) Glossar

(EL) ά

(EN) Glossary

(ES) Glosario

(ET) Snastik

(FI) Sanasto

(FR) Glossaire

(HR) Pojmovnik

(HU) Glosszrium

(IT) Glossario

(LT) Žodynėlis

(LV) Glosārijs

(MT) Glossarju

(NL) Verklarende woordenlijst

(PL) Słowniczek

(PT) Glossrio

(RO) Glosar

(SK) Slovnk

(SL) Glosar

(SV) Ordlista

Contact

CNECT-consultation-DSA@ec.europa.eu