This document has not been adopted or endorsed by the European Commission. Any possible measures indicated in this paper are the preliminary elements being considered by the Commission services, they do not preclude the measures to be finally considered in the Impact Assessment and may not in any circumstances be regarded as stating an official position of the Commission. The information transmitted is intended only for the entity to which it is addressed for discussions and for the preparation of the Impact assessment and may contain confidential and/or privileged material.

IMPACT ASSESSMENT ON ILLEGAL CONTENT ONLINE
STAKEHOLDER CONSULTATION:
INTERNET COMPANIES

Introduction:

In the context of the ongoing work on the Impact Assessment on Illegal Content Online, the Commission would like to get your views on a number of issues set out below. These views will complement the Open Public Consultation (OPC, available here), as well as the data collection exercise based on the table of indicators.

The Commission started work on an impact assessment outlining potential problems, objectives and options in the attached Inception Impact Assessment (IIA). As part of the options to be considered, the Commission will analyse the current situation (baseline scenario) as well as actions to reinforce the voluntary measures as well as possible sector-specific legislation (including in particular on terrorism content online) as well as horizontal legislation applicable to all types of illegal content.

The measures presented in the Inception Impact Assessment[1] are initial ideas, and additional actions and options could be considered. The actions to be undertaken would be mainly addressed to online platforms, but could also require further action by Member States.

In addition to the requests for factual data as part of the reporting exercise within the EU Internet Forum and the possibility to contribute to the Open Public Consultation that closes on 25th June, we would like to offer you the possibility of providing further input to the Impact Assessment by replying to **the questions below and provide any additional considerations in writing by 15th of June.** We are also available on the week of 18-22 June to hold a meeting or videoconference, at a time to be arranged, in order to discuss your input, clarify any questions you may have and discuss additional elements which you consider should be taken into account.

[1] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1183598_en

Questions

1. What are the main risks or concerns for your company as regards terrorist content online which could be hosted in your platform? Please indicate your agreement with the following statements, with a short justification to the extent possible.

Statement	Impact	Justification
Such content has a negative impact on our users	☐ Very negative ☐ **Negative** ☐ No impact ☐ I don't know	Many people treat it as a spam and simply don't read it. Some uses it as a source of information about war in Syria.
Such content damages the reputational image of the company	☐ Very negatively ☐ **Negatively** ☐ No impact ☐ I don't know	[redacted]
Such content impacts on the company's business model (e.g. risks of losing advertising or users switching to other platforms)	☐ **Very negatively** ☐ Negatively ☐ No impact ☐ I don't know	Company can have problems not only with advertisers, but also with payment processors (due to anti-terrorist laws) and other social platforms (which don't want to expose their users to such content).
Such content undermines the trust by users when using the Internet	☐ To a large extent ☐ To some extent ☐ **To a limited extent** ☐ Does not undermine trust ☐ I don't know	
Risks of litigation by hosting such content	☐ Is a serious concern ☐ **Is a concern** ☐ Is not a concern	
Risks of diverging legislation in different countries to address such content posing excessive regulatory burden on companies	☐ **Is a serious concern** ☐ Is a concern ☐ Is not a concern	The more distinct legislations are in this matter, the harder it will be for small platforms to comply with them. Single legislation across EU could be beneficial in this way.
Other; please elaborate: Risk of political propaganda being published the same way as terrorist propaganda today	**Is a serious concern**	There's a risk, that in future some state actors will try to publish political propaganda to destabilize situation across EU member states (like Russia is currently doing in Ukraine).

2. What measures could be developed to **reinforce the voluntary approach** (e.g. a Memorandum of Understanding or a Code of Conduct between the EU and the industry including specific commitments building upon the Recommendation[2])?

If some studies would be available about amount of terrorist content on different platforms it would help them to understand how their platform is being abused. Many platforms probably doesn't know about the scale of abuse and how they are abused.

3. Which actions could be taken to **support small companies** and start-ups in tackling terrorist content online effectively? Should these be taken by larger companies, public authorities or both?

Public authorities and larger companies should share information and tools with smaller platforms to inform them about abusive content and to share various information in this context.

Public authorities (like Europol) should provide high quality reporting of abusive content on the platform, as it's difficult for smaller companies to detect and understand abusive materials in many foreign languages.

Smaller platform should be able to get some form of handbook with instructions how to deal with terrorist content written in more friendly manner.

4. What are your views on **regulating at EU level in the following areas** and how would you qualify the **impact on your business (positive or negative)**? Please provide a short justification of your assessment.

Definition of terrorist content	Positive, it would be beneficial to have a single definition
Requirements regarding the companies' terms of service	Positive, if requirements would be reasonable
General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content	Positive, if measures would be reasonable. It would allow to avoid situation when some companies are removing this kind of content, and others don't have to. This requirement should be based on size of the platform (number of users / employees), and on the

[2] https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

(complemented by self regulation)	amount of propaganda published (some measures should be taken only on heavily abused platforms).
Specific requirements in terms of action upon referral (including time limit of one hour)	
More explicit and detailed obligations to deploy specific proactive measures (including automatic detection)	Negative (for smaller platforms). It's very hard to build a good law in this matter (e.g. copyrights infringements), but largest platforms should be obligated to deploy them in at least some extend along with reporting of effects.
Specific requirements to cooperate with other hosting service providers to avoid the dissemination across platforms	Negative (for smaller platforms). Many times this could be hard to implement. This should be more based more on voluntary approach.
Sanctions in case of non-compliance	EU should have power to block access to platforms that are not complying with most important requirements. This would be important in case of political propaganda used to destabilize member states.
Exchanges of information with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material	Positive, but should be forced only on largest or most abused platforms (not every platform contains terrorist materials). Amount of information provided should depend on the type of the platform and its size.
Clarify that companies engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)	Positive
Requirement to Member States to increase referral capabilities, quality criteria for referrals and for referral entities in Member States to provide relevant support to companies in case of doubt about qualification as terrorist content (e.g. through points of contact)	Positive, poor quality referrals do a lot of damage for the whole process
Nomination of point of contact within Companies	Positive, but for very small companies it could be illusionary

Reporting obligations for companies[3]	Positive, but only if the size of the platform will be taken into account during deciding how specific the reporting should be
Transparency requirements for companies vis a vis their users[4]	Positive
Compulsory safeguards, such as the ones in the general chapter of the Recommendation	Positive
The establishment of an external audit/monitoring mechanism for assessing compliance of companies.	Positive, but only if it wouldn't be very complicated to comply

[3] See point 41 of the Recommendation.
[4] See points 16 and 17 of the Recommendation.