

*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 Member State or 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: MEMBER STATES

### **Introduction:**

Following the initial discussion with Member States at the EU Internet Forum (EUIF), the Commission would like to get more detailed views on possible actions to more effectively tackle terrorist content online as part of the ongoing work on the Impact Assessment on Illegal Content Online. 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<sup>1</sup> 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.

Member States are kindly requested **to reply to the questions below and provide any additional considerations in writing by 13 June 2018**. The results of this questionnaire will be presented and discussed at the **forthcoming meeting on 15 June**. In parallel, the European Commission's Directorate-General for Communications Networks, Content and Technology convened its expert group under the eCommerce Directive also feeding into the work of the impact assessment.

---

<sup>1</sup> [https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1183598\\_en](https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1183598_en)

**Questions**

**I. Problem and baseline scenario**

1. What are the **provisions, arrangements etc under national law addressing the removal of terrorist content<sup>2</sup> for preventive purposes** (e.g. do you have duty of care provisions<sup>3</sup>, specific notice and action procedures, provisions on transparency of companies' actions in relation to the removal of terrorist content, provisions on safeguards, etc.)? Please indicate below – where relevant – the applicable laws or other legal documents.

Notice and action procedures	<p>The Law on Electronic Commerce on the Market (ZEPT) determines the way in the scope of electronic commerce on the market. From the point of view of information security, important articles defining the responsibility of the service provider or hosting provider for the data that are available over the network.</p> <p>Article 10: The court may order the service provider to stop or prevent an infringement. Notwithstanding the exclusion of the liability of the service providers referred to in the preceding paragraph, the court may order the removal or illegalization of illegal contents for the purpose of detecting and preventing criminal offenses, protection of privacy, protection of classified information and business secrecy. Such a proposal may also be referred to the court in the public interest for supervision by the competent administrative authorities, in accordance with the sectoral legislation.</p>
Transparency rules	
Safeguards	

Do you have **specialised entities that notify/refer terrorist content** to hosting service providers? What is the **legal basis and benchmark for notification/referral** (illegality of content, terms of service of hosting service provider)?

The Slovenian police established an EU IRU Contact Point (police officer - an analyst working in the field of terrorism). In its work, he also reviews Internet content related to terrorism, only for publicly available content.

In addition to this, the project of the NGO "(SPLETNO OKO) Web Eye" was

<sup>2</sup> For the purpose of this questionnaire, "terrorist content" is defined as in the Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final). <https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online>

<sup>3</sup> See recital 48 of the Directive on electronic commerce <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32000L0031>

launched in 2010, which can, in the context of monitoring and warning against hate speech on the World Wide Web, alert the police that certain elements of hate speech can be connected to or contain terrorist content.

Do you consider them **sufficient** in terms of preventing accessibility of terrorist content? What are the limitations?

For Slovenian situations where the level of terrorist threat is low and does not have major problems with radicalization (at least perceived) or publication of terrorism-related content, it is sufficient

2. Do you consider that the **amount of terrorist content online** in the last [two] years has overall

	Decreased substantially
X	Decreased
	Continued at the same level
	Increased
	Increased substantially

Please indicate the basis for your assessment. What do you think has contributed to this trend?

- military defeat IS  
- increased activity of Internet providers

3. Do you see a **risk that removal by companies** on their own initiative could **interfere with investigations or intelligence gathering**? What would be the **mitigating measures** necessary to address any such risks?

YES.

4. Do you see a risk of **erroneous removal** by platforms of legal content (e.g. removal of content misidentified as illegal, removal of content disseminated for research, educational or journalistic purposes, "over-removal")? Are you aware of **any cases** of over-removal? What would be the **mitigating measures** necessary to address any such risks?

There is a certain risk of withdrawal of content, which would mean an interference with freedom of expression and freedom of communication, but in principle this is not expressed in Slovenia

### Non regulatory options: reinforcing voluntary action

1. Do you think that the work under the **EUIF** as reinforced and complemented by the **Recommendation** is **sufficient** action at EU level to effectively tackle terrorist content online?

YES.

2. Do you consider that the **EUIF's work should be further developed** in order to reinforce action at EU level to tackle terrorist content online e.g. through a Memorandum of Understanding in which companies and possibly Member States would sign up to concrete commitments (see possible measures below)?

In principle for SI could be problematic regarding the MOU (not a proper – legally binding ground).

3. Which of the following **possible elements** should in your view be addressed and further developed within a voluntary approach? Please indicate the need from a scale from 1 (unnecessary) to 5 (very necessary)

2	More specific objectives for companies' actions (e.g. request a certain percentage of content taken down within a certain time limit)
4	Stronger commitments in terms of internal processes and resource allocation (e.g. to have certain procedures in place, conduct risk assessments and establish mitigating procedures, content of Terms of Service, training, capacity to detect content in different languages)
5	Standardised working arrangements between companies, law enforcement and Europol to enhance understanding of how platforms are abused, to improve referral mechanism, avoiding unnecessary duplication of efforts, facilitating requests from law enforcement agencies in relation to criminal investigations <sup>4</sup> .
4	Stronger commitment on specific proactive and preventive measures (i.e. further development and participation in industry-led schemes, such as the database of hashes developed in the context of the EUIF)

<sup>4</sup> See point 40 of the Recommendation.

1	More detailed requirements on transparency and reporting
2	More detailed requirements to companies on safeguards against over-removal
1	Establishment of an external audit/monitoring mechanism
3	Establishment of contact points, both in companies and Member States, to facilitate referrals (and feedback) and requests from law enforcement authorities in relation to criminal investigations.
2	Additional support (e.g. by Europol) to referral capacities in Member States

4. What other additional measures could be developed within a reinforced voluntary approach?

Raising public awareness of such issues and thus increasing their reporting of contentious issues.

5. Which further actions could be taken to secure participation from those **companies** who have **not engaged**?

--

6. Which further 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?

When terrorist content is detected and its provided by smaller Internet service providers, it enters the EU IRU (contact them, explain the problem, offer solutions and cooperation ... for example, JustPaste.it)

7. Do you think that the voluntary approach is **effective** and flexible enough to ensure that companies continue their efforts in the **long term**? Please indicate with which statement you would agree with:

X	Yes
	No, it should be reinforced as presented above to obtain sufficient guarantees
	No, it should be reinforced via legislation

## II. Legislative options

1. Why would you consider **legislation necessary at this time**? What would be the concrete benefits? What **risks** could legislation entail?

In Slovenia, we have the necessary legislation, which allows in the case of a criminal offense to submit a request for deletion of the content in question.

2. What should be the **material scope of legislation** (i.e. how should terrorist content be defined)? Do you consider that covering material inciting to commit terrorist acts (Article 21/Article 5 of the Terrorism Directive<sup>5</sup>) is sufficient or should the dissemination of material pursuing other terrorist purposes be included as well?

Material the dissemination of which pursues the following objectives should be included in legislative measures:

<input checked="" type="checkbox"/>	Recruitment for terrorism
<input checked="" type="checkbox"/>	Providing training for terrorism
<input checked="" type="checkbox"/>	Terrorist financing
<input checked="" type="checkbox"/>	Other, please elaborate: incitement to terrorism

To what extent should material produced by UN/EU designated terrorist organisations be included?

In any case we are sceptical with respect to legislative action, this is a matter of general legislative provisions (in Criminal Codes), also possible delimitations with hate speech, false news ... and the issue of protecting the freedom of expression and freedom of communications.

3. Which **measures** (based in particular on the elements mentioned in the Inception Impact Assessment) do you consider as **necessary elements of legislation** to be impactful? Please indicate the need from a scale from 1 (unnecessary) to 5 (very necessary)

	Definition of terrorist content ( <i>see question above</i> )
	Requirements regarding the companies' terms of service
	General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content (complemented by self regulation)
	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)
	Specific requirements to cooperate with other hosting service providers to avoid the dissemination across platforms
	Sanctions in case of non-compliance
	Exchanges of information with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material
	Clarify that companies engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)
	Requirement to Member States to increase referral capabilities, quality criteria

<sup>5</sup> Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA  
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0541>

	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)
	Nomination of point of contact within Companies
	Reporting obligations for companies <sup>6</sup>
	Transparency requirements for companies vis a vis their users <sup>7</sup>
	Compulsory safeguards, such as the ones in the general chapter of the Recommendation
	The establishment of an external audit/monitoring mechanism for assessing compliance of companies.

Do you consider that minimum requirements could usefully be complemented by self-regulatory measures? And if so, which ones?

Differently – we are sceptical about automatic self-detection measures. In any case – we would support more self-regulatory approach.

4. What **other additional measures** could be developed within legislation?

No other measures at the moment.

5. What should be the **personal scope of the legislation**? Only hosting service providers within the meaning of the Directive on electronic commerce or other service providers?

No position at the moment, but if legislative action is taken, probably wider (also other service providers), but in such cases the existing hosting exception(s) need to be still protected.

6. Do you think **smaller companies** should be covered by all obligations or should they be exempted from some of the obligations (e.g. proactive measures) but obliged by others (e.g. time-limits after referral)? Which companies could be partially exempted and from which obligations?

7. How do you see the **impact on fundamental rights** of the above-mentioned measures and which safeguards would be necessary to avoid undue interference with fundamental rights?

<sup>6</sup> See point 41 of the Recommendation.

<sup>7</sup> See points 16 and 17 of the Recommendation.