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[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.

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.

[1] 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[2] for preventive purposes** (e.g. do you have duty of care provisions[3], 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	MINISTRY OF JUSTICE: The primary legal basis can be found in Section 5 para 1 of Act No. 480/2004 Sb., on certain services of information companies: A provider of service, which consists in storing information provided by a user is responsible for the content of the information stored at the request of the user, only if a) if, having regard to the subject-matter of its activities and the circumstances and nature of the case, could have known that the contents of the information or acts of the user are unlawful; or b) if he or she becomes manifestly aware of the unlawful nature of the content of the stored information or of the user's unlawful conduct and has not immediately taken all steps that may be required to remove or disable such information. MINISTRY OF THE INTERIOR: Criminal Code imposes an obligation to report commission/suspicions of committing a terrorist offense (otherwise it may be a criminal offense - Section 368 Non reporting of Criminal Offense)

[2] 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

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

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)?

National Headquarters against Organized Crime (hereinafter "***NCOZ***") within the framework of Police of the Czech Republic.

NCOZ plays role of the national contact point for cybercrime, national contact point for reporting illegal content, as well as it is coordinator for the EU Code of Conduct.

One of the tasks of NCOZ is the prevention of terrorism. As regards referral to hosting service providers, NCOZ deals solely with content which is deemed to be illegal.

Hosting Provider Terms and Conditions: Act No. 480/2004 Sb., on certain services of information companies

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

MINISTRY OF THE INTERIOR:

Effective co-operation between law enforcement and private companies, especially hosting companies, is important in order not only to eliminate content but also to effectively investigate criminal offenses.

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

	Decreased substantially
	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?

MINISTRY OF THE INTERIOR:

Same level.

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?

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?

II. 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?

EUIF
- It is sufficient.

Recommendation
- z materiálu **Doporučení Evropské komise o opatřeních pro efektivní boj proti nezákonnému obsahu na internetu (on-line), popis problematiky a stanovisko ČR,** *C(2018)1177 z 1. 3. 2018,* autor MPO*:*

"ČR nepodporuje další prohlubování unijní harmonizace v oblastech terorismu nebo dětské pornografie, neboť má za to, že již existuje dostatečně fungující právní rámec nastavený dílčími předpisy a vhodně doplněný nelegislativními iniciativami. Důležitá je efektivní spolupráce orgánů činných v trestním řízení a soukromých subjektů, zejména s hostingových společností, aby nedocházelo pouze k odstraňování obsahu, ale rovněž k efektivnímu vyšetřování spáchaných trestných činů. ČR podporuje kodex chování pro boj proti nezákonným projevům nenávisti online,který měl pozitivní efekt na lepší spolupráci s většinou poskytovatelů hostingových služeb (teď se odstraňují 2/3 nezákonného obsahu). Máme za to, že je třeba ještě delší časový prostor k tomu, aby se vyhodnotilo, zda je stávající systém založený na „soft law" přijatelný, či zda je třeba přistoupit k legislativním krokům."

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)?

X

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)

	More specific objectives for companies' actions (e.g. request a certain percentage of content taken down within a certain time limit)
	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)
	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[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)
	More detailed requirements on transparency and reporting
	More detailed requirements to companies on safeguards against over-removal
	Establishment of an external audit/monitoring mechanism
	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.
	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?

MINISTRY OF JUSTICE:

It would be beneficial if IT companies such as Facebook or Google made public precise numbers as regards their teams dealing with illegal content online. E.g. how many lawyers/psychologists and other professionals is in reality determined to fight with this phenomena.

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

MINISTRY OF JUSTICE:

Moderate pressure from Commission towards IT companies (if it is not already in place).

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?

MINISTRY OF JUSTICE:

Commission could organise joint workshops for "big" IT companies and smaller

[4] See point 40 of the Recommendation.

enterprises, where experiences could be shared.

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

III. Legislative options

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

Czech Republic does not support any further harmonization on EU level in this matter. See our position on page 5 of this document.

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[5]) 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:

	Recruitment for terrorism
	Providing training for terrorism
	Terrorist financing
	Other, please elaborate:

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

[5] 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

X

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 (*see question above*)
	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 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[6]
	Transparency requirements for companies vis a vis their users[7]
	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?

X

[6] See point 41 of the Recommendation.
[7] See points 16 and 17 of the Recommendation.

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

X

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?

X

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?

X

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?

X