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	**General: S**everal provisions of German Law establish rights to demand the removal of illegal content from host providers. After notifying the host provider and providing it with knowledge of specific illegal content, the host provider – if not removing the content – loses its liability exemption as provided for by Article 14 (1) E-Commerce-Directive (Section 10 Telemedia Act - TMG). In such cases, Article 14 (Section 10 TMG) does not establish barriers for the right to demand removal and courts might order them to do so. German Law also establishes – under certain circumstances – the right to demand not only the removal of specific content, but also the prevention of similar instances of content in the future. All German courts have so far seen this as compatible with Article 14 (1) of the E-Commerce-Directive arguing that Article 14 (3) E-Commerce-Directive (Section 7 (2) TMG old version; now with slight amendments in Section 7 (3) TMG), allows for corresponding injunctions. The courts have seen this also in line with Article 15 (1) E-Commerce-Directive because the injunctions only create specific – not general – monitoring obligations. State Media Authorities can order the removal of certain illegal content directly from host providers according to Section 59 (4) of the Interstate Broadcasting Treaty (Rundfunkstaatsvertrag - RStV) and Section 20 (4) of the Interstate Treaty on the protection of minors (Jugendmedienschutzstaatsvertrag – JMStV). Deletion orders can in principle also be issued by police authorities, the legal basis for this being the general provision of the police to ward off danger (polizeiliche Generalklausel). **NetzDG:** Germany passed the Act to improve Enforcement of the Law in Social Networks (Netzwerkdurchsetzungsgesetz – NetzDG), which entered into force on 1 Oct. 2017. The act introduces compliance

[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

	obligations for social networks when dealing with take down notifications (user complaints) concerning illegal third party content. The act is only applicable if the illegal content fulfils the elements of specific offenses of the German Criminal Code (Strafgesetzbuch – StGB), as enumerated in Section 1 (3) NetzDG. Next to offenses from the category "hate crime" offenses are covered that can be classified as promotion of terrorism. For example, dissemination of propaganda material of unconstitutional organisations (Section 86 StGB), preparation of a serious violent offence endangering the state (Section 89a StGB) and forming terrorist organisations (Sections 129, 129a StGB) are covered. Amongst other things, the law requires social networks to take down or block unlawful content within 24 hours of receiving a complaint, if the content is manifestly unlawful, within 7 days in general if the content is unlawful. Systemic and culpable failures when dealing with complaints can result in fines of up to 50 million euro. Addressees of the law are social networks. The act excludes journalistic platforms or platforms meant for individual communication (mail and messenger services) or the distribution of specific content from its application. Professional networks and portals, online games and sales platforms are not included in the scope of application. Certain provisions of the law (e.g. the important compliance rules how to deal with user complaints which might be seen as a concretion of notice and take-down) do not apply for social networks with less than two million registered users in Germany. An English translation of the NetzDG is available at https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/NetzDG.html.
Transparency rules	In accordance with Section 2 Subs. 1 NetzDG providers of social networks (with more than 100 complaints per calendar year about unlawful content and more than 2 million registered users in Germany) are obliged to publish half-early reports on the handling of complaints about unlawful content. There are minimum requirements that need to be listed in the reports. Amongst other things, the reports shall cover i) the criteria applied in deciding whether to delete or block the unlawful content ii) number of incoming complaints about unlawful content, broken down as to whether complaints were submitted by users or complaint bodies and the reason for the complaint and iii) number of complaints that resulted in the deletion or blocking of the content, according to the reason for the complaint In addition, according to Section 3 Subs. 2 no. 5 NetzDG the providers of social network shall immediately notify the person submitting the complaint and the user whose content was reported about any decision about a reported content, while also providing them with reasons for its

	decision.
Safeguards	The NetzDG provides for the following safeguards: □ Narrow and clearly defined scope: Only specific content is covered, in line with specific criminal provisions set down in the Criminal Code. □ Only systematic non-compliance with the obligations to take-down content following a user complaint can lead to a sanction. A single wrong decision which does not follow from systematic failure to implement an effective complaints management cannot lead to a sanction. □ Flexible deletion deadlines: operators of social networks are required to remove manifestly illegal content within 24 hours, and in other cases (illegal, but not manifestly illegal) in general within 7 days. The timeframe of 7 days may be exceeded if the legality of the content in question depends on the veracity of a statement of facts or on other factual circumstances; in these cases the operator may give the user in question the opportunity to comment. □ Possibility to refer a take-down decision to self regulatory bodies: Networks have the option of referring difficult decisions regarding deletion to recognised institutions of regulated self governance and accepting their verdict. It is then not possible to impose a penalty on the basis of the Network Enforcement Act. □ A penalty can be imposed only if the networks are culpable of breaching compliance regulations. □ Preliminary court ruling: If the authority responsible for issuing fines aims to base its decision on the unlawfulness of undeleted content, a judicial verdict on the unlawful nature of the content should first be obtained, i.e. before a fine can be imposed, the authority should submit to a preliminary court ruling.

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)?

Complaints about illegal content online in general can be submitted by any natural person or legal entity to different players, these being i) State Media Authorities and hotlines, such as jugendschutz.net, ii) internet-beschwerdestelle.de, a self-regulatory body and trusted flagger. After juridical examination, these entities will notify the relevant host or access providers for the removal of the content (notice and take down

procedure) Please note that these entities do not specialise in flagging terrorist content, but often have their main focus on other youth-endangering content.

The Federal Criminal Police Office (BKA) is amongst other duties responsible for reporting/notifying terrorist online content to hosting service providers. In general the BKA uses the offered reporting channels to refer illegal content. An exception is YouTube, where the BKA is a member of the "trusted flagging program".

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

Germany is considering setting up a national Internet Referral Unit (IRU) within the Federal Criminal Police Office (BKA). At the moment the BKA already functions as competent authority but there is no independent division with IRU tasks.

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
X	Increased
	Increased substantially

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

The BKA has observed an increase in incriminated content in mid 2015. First observations indicate a minimal decrease after the commencement of the NetzDG.

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?

The immediate deletion of illegal content online can destroy evidence of a criminal offence and therefore influence criminal prosecution, the prevention of danger,

assessment and analysis duties of security agencies. However, it is likely that the immediate removal can help to prevent radicalisation processes, the circulation of unlawful online content, the building of crime related / terrorist networks.

So, to mitigate such risks it is absolutely necessary that the hosting service providers retain deleted content for a certain period of time. Furthermore, online-removed data must be made easily and fast available for security agencies.

The NetzDG introduces a solution in that context. According to the NetzDG, the big social networks have to make sure that in the case of removal, they retain the content as evidence and store it for this purpose within the (territorial) scope of Directives 2000/31/EC and 2010/13/EU for a period of ten weeks.

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?

Legal mechanisms shall provide safeguards to neutralize the risk of overblocking. The NetzDG is a good example in that case, because we see no evidence at practical level that the NetzDG is causing over-removal (see answers to question I.1.).

There must be a legal mechanism for users whose posts are wrongly deleted to appeal to get them reinstated.

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?

We think that the Recommendation is a first and important step in the process. Also the NetzDG in Germany has shown progress regarding the removal of illegal content online. However the last company reports within the EU Internet Forum have shown that the voluntary efforts of the companies regarding **terrorist** online content are not enough. For example only 13 of 33 companies responded to the table of indicators and removal times after notice are still too long.

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)?

Yes, the EUIF's work should be further developed.

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)

4	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)
4	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].
5	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)

[4] See point 40 of the Recommendation.

5	More detailed requirements on transparency and reporting
5	More detailed requirements to companies on safeguards against over-removal
5	Establishment of an external audit/monitoring mechanism
5	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.
4	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?

- Incentives for voluntary measures, such as a balanced good-samaritan-priciple (meaning that knowledge of infringing material gained through voluntary measures does not create an unfair risk of liability).
- Establishment of special reporting channels for public authorities.
- Any rules and procedures that self-regulatory body members are required to follow must comply with basic principles of due process.

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

Legal obligations would help to engage more companies.

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?

SMEs may have fewer capacities to remove terrorist online content. SME's might also not be able to install intelligent filter systems as they technically do not work on the systems of smaller platforms. That's why we need a balanced approach that considers the number of users and the worldwide consolidated turnover of the companies especially for the European SMEs. This means company obligations and sanctions must be proportionate.

There should be a closer cooperation of larger companies with smaller companies for example in the frame of Global Internet Forum to Counter Terrorism (GIFCT).

However there might be a risk that small platforms will become more dependent from certain big platforms that are market players and that their market power will be unintentionally manifested.

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:

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

Due to the NetzDG in Germany the cooperation with the internet service providers has improved. That's why Germany would also prefer to consider legislation on countering terrorist content on EU level without prejudice to the provisions in Directive 2000/31/EC on electronic commerce.

Legislation could improve legal security for internet service providers as well as for internet users. It may also lead to an even higher engagement of companies and stronger incentivise the establishment of a well-functioning complaint-system (Notice & Action).

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:

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

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

same scope

[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

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)

5	Definition of terrorist content (*see question above*)
4	Requirements regarding the companies' terms of service
5	General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content (complemented by self regulation)
5	Specific requirements in terms of action upon referral (including time limit of one hour)
4	More explicit and detailed obligations to deploy specific proactive measures (including automatic detection)
5	Specific requirements to cooperate with other hosting service providers to avoid the dissemination across platforms
5	Sanctions in case of non-compliance
5	Exchanges of information with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material
4	Clarify that companies engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)
4	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)
5	Nomination of point of contact within Companies
5	Reporting obligations for companies[6]
4	Transparency requirements for companies vis a vis their users[7]
5	Compulsory safeguards, such as the ones in the general chapter of the Recommendation
4	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?

Yes, in principle. However it needs a thorough examination, in how far self regulatory measures can be sufficient. An advantage could be the greater flexibility and openness for (technical) development.

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

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

- Legislation on EU level without prejudice to the provisions in Directive 2000/31/EC on electronic commerce.
- Balanced approach which considers the size of the companies (especially European SME) regarding obligations and sanctions.
- Horizontal approach to tackle illegal content online by implying Notice and Action procedures for all kinds of illegal content but taking account of the risk potential of the illegal content in question (i.e.: terrorist content, pedo-pornographic content).

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?

Only hosting providers within the meaning of the Directive on electronic commerce.

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?

A balance between big companies and SME needs to be struck, so exemptions for some of the obligations are necessary and adequate. Also the principle of proportionality must be taken into account. (see also answer to question II. 6.)

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?

- improvement of user rights, contractual claim of affected users to have blocking decisions reassessed

- final decision by an independent body whether a certain content is illegal or not

- clear and narrow scope of affected content

- transparency towards user and reporting person about reasons for take-down decision

- transparency reports on number of complaints and take-downs

- in case of fines for non-compliance: fines only for systemic failures of platforms