# Position Paper

## Position Paper on the Regulation on preventing the dissemination of terrorist content online

30.10.2018



**Summary**

The European Commission published proposal COM (2018) 238 final for a 'Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online', on 12 September 2018 ('Regulation'). Prior to the proposal, the Commission published its 'Recommendation on measures to effectively tackle illegal content online' on 1 March 2018, building on the Commission Communication of September 2017. The Recommendation outlined a number of measures to stem the uploading and sharing of terrorist propaganda online, which are taken on in the proposal for the Regulation.

Bitkom welcomes the proposal´s aim to improve the effectiveness of the fight against terrorist content online. It is beyond doubt that terrorist content is unacceptable – offline and online. The liability regime for illegal content determined in the e-Commerce Directive ('eCD') and refined in several judgments is well-engineered, balanced, and sufficient to address contemporary challenges regarding illegal content online. Providers of hosting services are obligated to act expeditiously under well-defined circumstances in order to avoid liability. Beyond that, many service providers voluntarily take action in order to enforce their own community policies. Working with rigid legal obligations and fixed deadlines coupled with high penalties, as demanded in the proposal, is dangerous and probably even counterproductive, as they could lead to wrong decisions and overzealous removals. The proposed Regulation presents a severe intervention in the companies' business model and therefore requires solid justification. However, the impact assessment of the European Commission does not properly assess the impact of this specific legislation on industry, especially on SMEs. For the reasons specified in the following paper, Bitkom urges the legal services of co-legislators to carefully review the legal grounds of this Regulation.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

**Marie Anne Nietan**
**Media Policy**
P +49 30 27576-221
m.nietan@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

bitkom

## Content

Page

## 1 The responsibility of hosting service providers

Bitkom supports the fight against the dissemination of terrorist content online and advocates for the prosecution of crimes in this area. Members of Bitkom explicitly stand by their responsibility to offer their support in this fight. Many service providers already voluntarily take action in order to enforce their own community policies.

We welcome the Commission's intention to improve the cooperation between private companies and competent authorities. The application and enforcement of applicable law is the responsibility of authorities and courts. Bitkom supports the voluntary involvement of social network operators in law enforcement, for example by providing mechanisms for marking and reporting posts and deleting relevant content. However, the enforcement of law on the Internet could in particular be improved by tackling the root of the evil; namely those who create terrorist content and publish and distribute it on social networks. Appropriate deterrence can only be achieved through consistent prosecution. Bitkom explicitly supports companies to provide assistance here. Bitkom members want to express their openness to working together to develop proposals that enhance cooperation between companies on the one hand and law enforcement agencies and courts on the other.

Self-regulatory and co-regulatory measures have established themselves as very effective tools in the media policy context. Even in the text of this specific proposal, the Commission acknowledges that progress has been made in tackling terrorist content through voluntary framework partnerships put in place by hosting service providers. These positive experiences should be taken into account in this proposal. The proposal addresses regulatory issues that are difficult to grasp and aims at the cooperation of different actors who are very likely to have different practical implementation requirements. In such a heterogeneous environment, self-regulatory and coregulatory approaches have proven to be successful, since legislators define the socially and regulatory necessary framework conditions, while the respective actors can develop relevant implementations for the practice.

With the aim of engaging constructively in the legislative process, we would like to comment on the proposal for a Regulation as follows:

## 2 Summary of concerns

Several issues of the proposal are of concern:

- Factual justifications behind the measures are lacking. No facts are provided as to specific problems encountered with take down activities of the past. Stakeholder consultations referred to in the explanatory memorandum of the proposal have been targeted at illegal content in general without a focus on terrorist content. We urge the Commission to conduct a proper impact assessment on the real need for this Regulation.

- The scope of the Regulation is extremely broad and lacks precision as well as clarity. It might apply to all hosting service providers, which encompasses not only social networks but any platform and communication service which hosts data of third parties, including all cloud service providers, including cloud infrastructure services, which do not control their customer's data.

- Without proven necessity, all service providers are forced to set up infrastructure allowing for rapid examination and removal of content, proactive measures including upload filters, annual reports and a 24/7 point of contact. This approach is lacking proportionality since an enormous (financial) effort is imposed on multiple companies without a concrete occasion being given.

- It is unclear, how 'competent authorities' will be appointed. It is also unclear, to which extent these authorities' competences must be extended by national law in order to fulfil the functions envisaged in the proposal. It has to be clear for the hosting service providers which authority is responsible for them. Therefore, each Member State should have a single judicial authority responsible.

- The proposal fails to clarify the rationale behind the distinction between removal orders and referrals. It is unclear how and for which reasons a competent authority would choose either of those two mechanisms.

- The proactive measures envisaged by the Regulation to be taken by hosting service providers include the use of automatic tools to detect and remove terrorist content - this is not compatible with the eCD, which prohibits the imposition of a general obligation on service providers to monitor the information they transmit or store.

- The implementation of complaint mechanisms for removal orders, referrals and proactive measures is very costly and time intensive, especially for SMEs. In addition, this risks establishing a general right to upload any content, which should be prevented.

- With regard to penalties, it is unclear which authority may level fines and how these are designed. It is not defined whether infringements must be systematic in order to be punishable by a fine. Penalties of up to 4% of global turnover for failure to comply with very short deadlines without clarifying the nature, gravity and duration of non-compliance are disproportionately high.

- The combination of extremely short deadlines for content removal and high penalties leads to an incentive to delete content without examining it thoroughly. The deadline for deletion of one hour after receipt of the removal order is far too short to examine the content. This is of concern with regard to fundamental rights enshrined in the Charter of Fundamental Rights of the European Union ('CFR'), such as freedom of expression and information.

# 3 Subject matter and scope of the Regulation (Article 1 and 2)

## 3.1 Definition of 'hosting service provider'

According to Article 1 (2), the Regulation applies to 'hosting service providers offering services in the Union, irrespective of their place of main establishment'. As a consequence, the Regulation applies to all hosting service providers in the same way without exceptions being made for small companies or those based outside the European Union. This is concerning since especially small and medium sized companies are lacking the (financial) resources to set up the infrastructure demanded by the Regulation.

In Article 2, a 'hosting service provider' is defined as 'a provider of information society services consisting in the storage of information provided by and at the request of the content provider and in making the information available to third parties'. This definition is too broad and lacks precision. Expressed this way, it could include cloud services, E-mail services, instant messenger services, web hosters, social media, appstores, marketplace, professional networks (i.e. Linkedin/Xing), news websites with comment functions and software development services. By focusing on third party access instead of access to the public, all cloud infrastructure providers, including those offering business to business

hosting services or privately shared cloud services are included in the scope of the Regulation.

Bitkom urgently calls on legislators to limit the scope of the Regulation, excluding providers that do not provide access to the public. It is important for the protection of the overwhelming majority of law abiding users to protect the privacy when sharing material on a private cloud service which are explicitly designed not to be accessible to the public. This right to privacy and data protection has to be carefully balanced against the danger of dissemination of terrorist content online.

Furthermore, providers of business to business hosting services should be excluded from the scope. Those providers are, most likely, not able to take down specific content since this would entail taking down entire public services that rely on their infrastructure. Business to business cloud infrastructure providers typically do not have access to the data stored in the cloud in a way which would allow them to monitor or filter illegal content and control the data that is made public.

## 3.2 Definition of 'terrorist content'

The definition of 'terrorist content' given in Article 2 (5) of the proposed Regulation is too vague and offers too much interpretational leeway. In order to be able to effectively and swiftly remove terrorist content, hosting service providers will need both consistent interpretations of what constitutes 'terrorist content' from competent authorities when they issue removal orders and guidance for industry on how to interpret 'terrorist content' when reviewing referrals or exercising proactive take-down measures. It is unclear who takes the final decision in case of doubt over whether the content can be classified as terrorist - this cannot be left to the discretion of the provider but has to be more clearly defined in Regulation.

# 4 Competent authorities

According to Article 17 of the proposal, Member States shall designate the authorities competent to issue removal orders and referrals, oversee the implementation of proactive measures and enforce obligations through penalties. It is, however, entirely unclear, which and how many authorities will be vested with the powers described in the proposed Regulation, such as issuing removal orders and referrals. This has to be more narrowly defined

and the number of authorities has to be restricted in order to create legal certainty for the affected companies on which authority is responsible for them. Each Member State should have a single judicial authority responsible for companies having their seat or being otherwise (principally) established in the authority's member state - it should not be possible for any authority to act on any company.

The proposal does not explain whether some authorities' powers need to be extended in order to be capable of overseeing and enforcing the obligations under the proposed Regulation. Some powers attributed to the competent authorities by the proposed Regulation appear too broad. For example, the discretion to determine whether the proactive measures taken by the hosting service providers are sufficient and the power to issue a request to take additional measures attributed to the competent authority by Article 6 (3) should lie with a judge.

## 5 Removal orders and referrals

The handling of removal orders as well as the establishment of measures for handling referrals as foreseen in Article 4 and 5 respectively creates an enormous effort for the companies. Considering the broad scope of the Regulation and how many companies will be affected, this effort is not proportionate to the added value it can bring, considering that it would also impact on a lot of companies that do not have any issues with (the deletion of) terrorist content. In addition, there should be a process in place for companies to challenge removal orders and referrals based on doubts as to their compatibility with fundamental rights.

### 5.1 Removal orders according to Article 4

Undoubtedly, terrorist content online has to be removed without undue delay upon acquiring knowledge thereof. The appropriate time frame and measures to acquire said knowledge depend on the type of content and the type of infringement. The measures to execute notice-and-take-down-procedures are continuously being developed and improved upon. The deletion deadline of one hour after receipt of the removal order given by the proposed Regulation is too short. Any obligation to react within such a short time after receiving a notice brings with it the danger of taking wrong decisions and removing content to pre-empt potential penalties – ultimately resulting in overblocking, running counter to the fundamental rights of citizens. Notwithstanding, any deadline for deletion

should be focused on the moment the company gains knowledge of the order and not the moment of receipt – as demonstrated in the liability concept of the eCD (Article 14 (1).

It is not possible to have all content examined by human employees within a one-hour time frame, meaning that this process might have to be carried out by automated means. Such measures place the existence of smaller businesses in jeopardy, which cannot afford to have mechanisms installed that allow such a rapid reaction.

In its Recommendation C(2018) 1177, the Commission justifies the short deadline for deletion by asserting that terrorist content is most harmful in the first hour after it appears online. This claim is not convincing. Content on social networks becomes more popular through increasing interactions. Reactions to published content typically do not reach their peak within the first hour after publication. Therefore, the requirement to remove illegal content within such a short timeframe appears unjustified. In addition, the Commission does not seem to concentrate on the reach of the content in its formulation of the scope of the Regulation since it does not restrict it to hosting service providers with a broad public reach.

We suggest to discard the one-hour-rule and return to the more flexible term '*without undue delay*', as used in no. 34 of Recommendation C(2018) 1177. This term clearly states the intention of the legislator to entice a swift reaction on part of the particular provider, yet leaves room to distinguish between the needs and capabilities of both large and small businesses.

In the context of the one-hour deadline, the question arises how it can be guaranteed that competent authorities are able to detect terrorist content fast enough (right when it is published in order to guard the one hour rule) and act on it immediately. If this is not given, the one-hour-rule loses its justification since the first hour after upload could be over at the time the authority orders to remove the content. In addition, it is not entirely clear how the competent authorities can guarantee a high quality standard in their examinations and orders. This is at least as crucial as the guarantee of efficient responsiveness as well as good work on part of the hosting service providers.

## 5.2 Repeated reports according to Article 4 and 6

The existing framework proposed in Article 4 (9) would see repetitive reports from hosting service providers to competent authorities, since every time a removal order becomes final, the authority that issued the order must inform the authority overseeing the provid-

er's proactive measures under Article 17(1)(c). Under Article 6(2), once the second authority receives this notification, it must ask the provider to report on the proactive measures it has taken to deal with terrorist content (in general, not just the specific content covered by the removal order). It appears that the second authority must make such a request every time it receives a notification under Article 4 (9). The provider must then report back to the second authority 'within three months after receipt of the request and thereafter at least on an annual basis.' This implies that providers must report within three months of every request under Article 6 (2), and if a provider has ever received such a request, it must thereafter report at least annually, even if it has received no further requests in that period. Consequently, this would place undue operational burden on both the hosting service providers and the second authority; the former having to repeatedly provide largely identical reports in response to separate requests, the latter being forced to make repeated requests for the same report.

We would therefore recommend devising a more pragmatic procedure to scale down the potential number of reports generated. If there are no relevant updates to the proactive measures being taken to deal with terrorist content, Article 6 (2) might allow hosting service providers to refer a competent authority to a previously submitted report.

## 5.3 Referral according to Article 5

The proposal requires all hosting service providers to set up 'operational and technical measures facilitating the expeditious assessment of content that has been sent by competent authorities'. The establishment of these measures can only be realized with considerable additional expenditure on part of the companies. Due to the broad scope of the proposed Regulation, all providers on whose systems user-generated content can be stored would be obliged to provide a qualified service for monitoring incoming referrals. Especially smaller providers would unreasonably suffer from such a resource-intensive obligation. In addition, many social media platforms already make use of 'trusted flaggers'.

By requiring hosting service providers to assess the content identified in the referral and to take the decision on whether it has to be removed, the proposal shifts the law enforcement to private institutions. This shift is especially concerning when taking place within the area of the fundamental rights to freedom of expression and information. Hosting service providers are subject to stricter obligations than courts and do not have a neutral stance since they are involved themselves. Yet, a quasi-judge role is imposed on the hosting service providers by the proposed Regulation. If content is deleted as a result of a referral, its decision has a similar effect as a judgment. However, the hosting service provider in

no way meets the requirements demanded from a court. They are under great social pressure while courts, on the other hand, are neutral and must be protected from social pressure. The deletions by the social networks affect their own business model. They become 'judges in their own right' and can hardly act neutrally. It is furthermore unclear who will be liable for the removal – the hosting service provider itself or the competent authority that issued the referral. The Regulation should in any event clearly exempt the hosting service providers from the liability of having taken down legitimate content that has been falsely erased under the pressure of rigid deadlines and heavy fines. Conversely, if a hosting service provider decides against removing content raised in a referral due to the various reasons outlined above, Article 5 remains unclear as to whether the respective hosting service provider could face liability for non-compliance. Where the competent authority chooses to address a referral rather than a removal order, any decision taken by the online content service provider pursuant to the referral should not result in losing the benefit of the liability exemption provided for under the eCD.

Thus, Article 5 should clarify that the hosting service provider will not face liability or be subject to penalties by the referrer for deciding not to remove or block the content referred where it has reasonable grounds to do so.

## 5.4 Lack of clarity with regard to the distinction between removal orders and referrals

It cannot be inferred from the text of the proposal, in which cases the authorities will send a referral instead of a removal order and vice versa. The relevant content is in both cases of terrorist nature so it is difficult to comprehend for which reasons a softer or harsher instrument would be chosen. It is, however, essential that hosting service providers concerned are able to comprehend the authorities' reasoning since one measure is punishable by a fine while the other is not and therefore has different consequences for the company. More generally, to understand the rationale of the Regulation as a whole, it is important to comprehend the intention of the lawmaker behind this distinction. This is not given by the proposal as it stands now.

In order to facilitate the distinction between removal orders and referrals for both competent national authorities and hosting service providers, an indication of the threshold at which a removal order is appropriate should be included. Key factors could include: (i) whether the content is clearly and unambiguously terrorist content, and (ii) its actual, expected and/or potential reach. This would help achieve the Regulation's goal of creating

a 'harmonised system of legal removal orders' by ensuring that designated authorities across Member States take a similar approach to issuing removal orders.

## 6 Imposition of specific proactive measures according to Article 6 (4)

Article 6(3) allows a Member State competent authority, where it assesses that a provider's proactive measures are insufficient in mitigating and managing the risk and level of exposure, to request a provider take specific additional proactive measures. The hosting service providers will have limited recourse to appeal such decision - under Article 6(5), the authority can only be asked to revoke its decision, but there is no provision for an appeals process to any other body. We are concerned that this provision might allow national authorities to impose a technology mandate. These specific technical requirements are infeasible, impractical or even counter-productive since they are likely to be a disincentive for companies to develop state-of-the art measures to detect and remove terrorist content. Instead, companies will wait until Member States propose and impose the requirement, including solutions that may not be technologically feasible or effective. Consequently, a formal appeal process to an external body (e.g. a dedicated panel or court in the relevant Member State) should be established in case that the authority declines to revoke its decision and provide that an authority imposing additional measures must take into account representations from the provider.

## 7 Complaint mechanism according to Article 10

Article 10 (1) requires hosting service providers to 'establish effective and accessible mechanisms allowing content providers [...] to submit a complaint against the action of the hosting service provider' in case their content has been removed as the result of a referral or proactive measure. In principle, we welcome the idea for the proposed complaint mechanism since it strengthens the right to freedom of expression, as enshrined in Article 11 CFR. However, the legal requirement for the establishment of a complaint mechanism as envisaged in Article 10 of the proposed Regulation would lead to high costs and time expenditure on part of the companies. Especially small and medium sized companies could see their business placed in jeopardy. In addition, there is the risk that a general right to re-upload and then a general right to upload could be inferred from a legally anchored complaint mechanism. This should be prevented.

In addition, it is highly problematic that, according to the proposal, the complaints are to be directed at the hosting service provider and not at the authority, while the authority is the one that issues the referral.

## 8 Information Disclosure according to Article 13 (4)

Article 13 (4) of the proposed Regulation obliges hosting service providers to inform authorities competent for the investigation and prosecution in criminal offences where they become aware of any evidence of terrorist offences. Bitkom explicitly advocates the investigation and prosecution of any criminal offence on the internet, especially in relation to terrorism. However, it is highly problematic that the proposed Regulation requires hosting service providers to inform on their own customers. Furthermore, the provision risks putting service providers in the untenable position of assessing information on 'terrorist offences'. A clear threshold should be set requiring the notification of law enforcement authorities only when terrorist content poses a direct threat to life or safety or is clear evidence of a terrorist offence. Such a threshold would ensure operationally a proportionate and manageable volume of notifications for hosting service providers and authorities.

## 9 Point of contact according to Article 14

The establishment of a point of contact to handle requests at any time will only be possible with considerable financial effort on part of the companies. Therefore, at least, the possibility must be given for companies to outsource the establishment of a point of contact to a third party.

It is unclear, how exactly the point of contact is envisaged to fit within the companies' structure.

## 10 Penalties

In general, it is not clear which competent authority may level penalties and how these are designed. Article 15(1) states that the Member State in which the provider's main establishment is located will have jurisdiction for the purpose of Article 18 (re penalties). However, Article 15(3) states that if an authority in another Member State issues a removal

order, that Member State has jurisdiction to take 'coercive measures' to enforce the order. Recital 34 refers to these as 'coercive measures of a non-punitive nature, such as penalty payments'. It is unclear whether these include penalties under Article 18(1) (b) for failing to comply with a removal order. If so, this would be the only exception from what otherwise appears to be a 'one stop shop' approach.

Member States are required to lay down rules on penalties applicable to infringements of obligations described in the proposed Regulation. It is not clear whether this infringement must be systematic in order to be punishable by a fine or whether a one-time infringement would be sufficient. The latter case would lack any proportionality considering the broad scope and rigid deadlines of the proposal. In addition, the provisions as they stand now could lead to varying penalties across Member States, leading to disproportionate outcomes.

Financial penalties with up to 4% of global turnover for systematic failure to comply with a fixed one-hour-deadline without clarifying the nature, gravity and duration of non-compliance are disproportionately high. In addition, the question arises as to how many individual infringements one must expect to be defined as a systematic failure to comply – this could again result in unharmonized assessments across Member States.

## 11 Entry into force

The Regulation shall apply from 6 months after its entry into force. Considering the obligation to establish a point of contact, complaint mechanism and proactive measures, this time frame is too short. Other Regulations usually define transitional periods of rather 18 months.

The German Ministry of Justice already needed more than 6 months to determine penalty guidelines for the German Netzwerkdurchsetzungsgesetz.

# 12 Compatibility with EU law

## 12.1 Compatibility with the Charter of fundamental rights

As the Commission admits in the explanatory memorandum, the proposal could potentially affect a number of fundamental rights – those of the content provider as well as those of the service provider.

The use of fixed deadlines coupled with high penalties is dangerous and probably even counterproductive, as they could lead to wrong decisions and overzealous removals. This causes chilling effects and threatens to negatively affect the content provider's freedom of expression, as well as the rights of all citizens to freedom of expression and information, as enshrined in Article 11 CFR.

The envisaged obligation for hosting service providers to preserve terrorist content which has been removed or disabled for 6 months is problematic with regard to the content provider's right to protection of personal data, as enshrined in Article 8 CFR, as well as existing EU privacy and data protection law.

When a competent authority issues a referral, the hosting service provider is forced to take a decision whether to delete the content based on the information provided by the competent authority. The proposed Regulation does not foresee any possibility for the content provider to explain himself. While in court normally all parties are heard, the right to be heard on part of the person making the statement is not respected in the context of a referral – a complaint can only be filed when the content has already been deleted. This threatens to infringe the right to good administration as enshrined in Article 42 CFR, which includes the right of every person to be heard before any individual measure which would affect him or her adversely is taken.

The proposed Regulation presents a severe encroachment on the business model of the hosting service providers. This encroachment is not a reaction to a detected problem but rather a pre-empting general obligation for all providers. This is problematic with regard to the service providers' right to freedom to conduct a business, as enshrined in Article 16 CFR.

The service providers' right to an effective remedy is restricted by the fact that removal orders can only be opposed to in case of force majeure, in case of de facto impossibility not attributable to the hosting service provider or in case the removal order contains manifest errors or does not contain sufficient information to execute the order.

For the reasons mentioned above, the Regulation should provide for a formal process to appeal to decisions taken by the competent authority at an external body.

## 12.2 Compatibility with the e-Commerce Directive (eCD)

Services considered information society services fall under the scope of the eCD. The current liability system determined in the eCD succeeds in striking a good balance for all parties. The liability regime of the eCD has proven itself strong and flexible. It has been aiming at promoting dynamic, competitive markets since its inception. Contributions of those intermediaries' services, as covered by the eCD's liability limitations, to the economy would not have been possible at current levels without the liability regime in this Directive. Within this liability framework, industry codes of conduct, self and co-regulation, and industry best practices have been developed to ensure a stable, well-regulated market. These different regulatory approaches are crucial to ensuring progress in the fight against illegal content while at the same time respecting fundamental rights.

According to Article 14 of the eCD, the notice-and-take-down procedure only covers specific content about which knowledge must be available on the part of the hosting service provider. A general and proactive monitoring obligation is expressly prohibited under Article 15 eCD. Whether the proactive measures provided for in Article 6 of the proposed Regulation meet these European legal requirements is highly questionable. It is not clear which kind of measures the Commission has considered here, which would not lead to a preliminary examination of the content uploaded to a network for its illegality. It is particularly concerning in this regard that the Commission explicitly mentions automated tools to detect and identify terrorist content as possible proactive measures. Consequently, a clarification on the interplay between the requirement for proactive measures in Article 6 of the draft Regulation and the hosting exemption in Article 14 of the eCD is required.

regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.