034673/EU XXVI. GP
Eingelangt am 14/09/18

Council of the European Union

Brussels, 14 September 2018
(OR. en)

12129/18

Interinstitutional File:
2018/0331(COD)

CT 144
ENFOPOL 450
COTER 114
JAI 881
CYBER 193
TELECOM 288
FREMP 142
AUDIO 64
DROIPEN 127
COHOM 107
CODEC 1468

PROPOSAL

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	12 September 2018
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2018) 640 final
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on preventing the dissemination of terrorist content online *A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018*

Delegations will find attached document COM(2018) 640 final.

Encl.: COM(2018) 640 final

www.parlament.gv.at

EUROPEAN
COMMISSION

Brussels, 12.9.2018
COM(2018) 640 final

2018/0331 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on preventing the dissemination of terrorist content online

A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018

{SEC(2018) 397 final} - {SWD(2018) 408 final} - {SWD(2018) 409 final}

www.parlament.gv.at

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

1.1. Reasons for and objectives of the proposal

The ubiquity of the internet allows its users to communicate, work, socialise, create, obtain and share information and content with hundreds of millions of individuals across the globe. Internet platforms generate significant benefits for users' economic and social wellbeing across the Union and beyond. However, the ability to reach such a large audience at minimal cost also attracts criminals who want to misuse the internet for illegal purposes. Recent terrorist attacks on EU soil have demonstrated how terrorists misuse the internet to groom and recruit supporters, to prepare and facilitate terrorist activity, to glorify in their atrocities and urge others to follow suit and instil fear in the general public.

Terrorist content shared online for such purposes is disseminated through hosting service providers that allow the upload of third party content. Terrorist content online has proven instrumental in radicalising and inspiring attacks from so-called 'lone wolves' in several recent terrorist attacks within Europe. Such content not only creates significantly negative impacts on individuals and society at large, but it also reduces the trust of users in the internet and affects the business models and reputation of those companies affected Terrorists have misused not only large social media platforms, but increasingly smaller providers offering different types of hosting services globally. This misuse of the internet highlights the particular societal responsibility of internet platforms to protect their users from exposure to terrorist content and the grave security risks this content entails for society at large.

Hosting service providers, responding to calls from public authorities, have put in place certain measures to tackle terrorist content on their services. Progress has been made through voluntary frameworks and partnerships including the EU Internet Forum which was launched in December 2015 under the European Agenda on Security. The EU Internet Forum has promoted Member States' and hosting service providers' voluntary cooperation and actions to reduce the accessibility to terrorist content online and to empower civil society to increase the volume of effective, alternative narratives online. These efforts have contributed to increased cooperation, improving responses by companies to referrals by national authorities as well as Europol's Internet Referral Unit, the deployment of voluntary proactive measures to improve automated detection of terrorist content, increased cooperation between the industry - including the development of the "database of hashes" to prevent known terrorist content from being uploaded on connected platforms-, as well as increased transparency in efforts. While cooperation under the EU Internet Forum should continue in the future, the voluntary arrangements have also shown their limitations. Firstly, not all affected hosting service providers have engaged in the Forum and secondly, the scale and pace of progress among hosting service providers as a whole is not sufficient to adequately address this problem.

Given these limitations, there is a clear need for enhanced action from the European Union against terrorist content online. On 1 March 2018, the Commission adopted a Recommendation on measures to effectively tackle illegal content online, building upon the Commission Communication of September[1] as well as efforts under the EU Internet Forum.

[1] Communication (COM(2017) 555 final) on tackling illegal content online.

www.parlament.gv.at

The Recommendation included a specific chapter identifying a number of measures to effectively stem the uploading and sharing of terrorist propaganda online, such as improvements to the referral process, a one-hour timeframe for responding to referrals, more proactive detection, effective removal and sufficient safeguards to accurately assess terrorist content.[2]

The need to enhance action in relation to terrorist content online has also been reflected in calls by EU Member States, and some have already legislated or have expressed plans to do so. Following a series of terrorist attacks in the EU and given the fact that terrorist content online continues to be easily accessible, the European Council of 22-23 June 2017 called for industry to “develop new technology and tools to improve the automatic detection and removal of content that incites to terrorist acts. This should be complemented by the relevant legislative measures at EU level, if necessary". The European Council of 28 June 2018 welcomed “the intention of the Commission to present a legislative proposal to improve the detection and removal of content that incites hatred and to commit terrorist acts”. Furthermore, the European Parliament, in its resolution on online platforms and the digital single market of 15 June 2017 urged the platforms concerned "to strengthen measures to tackle illegal and harmful content", and called on the Commission to present proposals to address these issues.

To address these challenges and in responding to the calls by Member States and the European Parliament, this Commission proposal seeks to establish a clear and harmonised legal framework to prevent the misuse of hosting services for the dissemination of terrorist content online, in order to guarantee the smooth functioning of the Digital Single market, whilst ensuring trust and security. This Regulation seeks to provide clarity as to the responsibility of hosting service providers in taking all appropriate, reasonable and proportionate actions necessary to ensure the safety of their services and to swiftly and effectively detect and remove terrorist content online, taking into account the fundamental importance of the freedom of expression and information in an open and democratic society. It also introduces a number of necessary safeguards designed to ensure full respect for fundamental rights such as freedom of expression and information in a democratic society, in addition to judicial redress possibilities guaranteed by the right to an effective remedy as enshrined in Article 19 TEU and Article 47 of the Charter of Fundamental Rights of the EU.

By setting a minimum set of duties of care on hosting service providers which includes some specific rules and obligations, as well as obligations on Member States, the proposal intends to increase the effectiveness of current measures to detect, identify and remove terrorist content online without encroaching on fundamental rights, such as freedom of expression and information. Such a harmonised legal framework will facilitate the provision of online services across the Digital Single Market, ensure a level playing field for all hosting service providers directing their services to the European Union and will provide a solid legal framework for the detection and removal of terrorist content accompanied by appropriate safeguards to protect fundamental rights. In particular, obligations for transparency will increase trust among citizens, and in particular internet users, and improve the accountability and transparency of companies' actions, including in respect to public authorities. The proposal also sets out obligations to put in place remedies and complaint mechanisms to ensure that users can challenge the removal of their content. Obligations on Member States

[2] Recommendation (C(2018)1177 final) of 1 March 2018 on measures to effectively tackle illegal content online.

www.parlament.gv.at

will contribute to these objectives, as well as improve the ability of relevant authorities to take appropriate action against terrorist content online and to combat crime. Where hosting service providers fail to comply with the Regulation, Member States may impose penalties.

1.2. Consistency with existing EU legal framework in the policy area

The present proposal is consistent with the acquis related to the Digital Single Market and in particular the E-Commerce Directive. Notably, any measures taken by the hosting service provider in compliance with this Regulation, including any proactive measures, should not in themselves lead to that service provider losing the benefit of the liability exemption provided for, under certain conditions, in Article 14 of the E-Commerce Directive. A decision by national authorities to impose proportionate and specific proactive measures should not, in principle, lead to the imposition of a general obligation to monitor, as defined in Article 15(1) of Directive 2000/31/EC towards Member States. However, given the particularly grave risks associated with the dissemination of terrorist content, the decisions under this Regulation may exceptionally derogate from this principle under an EU framework. Before adopting such decisions, the competent authority should strike a fair balance between public security needs and the affected interests and fundamental rights including in particular the freedom of expression and information, freedom to conduct a business, protection of personal data and privacy. Hosting service providers' duties of care should reflect and respect this balance which is expressed in the E-Commerce Directive.

The proposal is also consistent and closely aligned with the Directive (EU) 2017/541 on Combatting Terrorism, the aim of which is to harmonise Member States' legislation criminalising terrorist offences. Article 21 of the Directive on Combating Terrorism requires Member States to take measures ensuring the swift removal of online content limited to public provocation and leaving Member States the choice of the measures. This Regulation, given its preventative nature, covers not only material inciting terrorism but also material for recruitment or training purposes, reflecting other offences related to terrorist activities, which are also covered by Directive (EU) 2017/541. This Regulation directly imposes duties of care on hosting service providers to remove terrorist content and harmonises procedures for removal orders with the aim to reduce accessibility to terrorist content online.

The Regulation complements the rules laid down in the future Audiovisual Media Services Directive insofar as its personal and material scope are broader. The Regulation does not only cover video sharing platforms but all different kinds of hosting service providers. Moreover, it covers not only videos but also images and text. Furthermore, the present Regulation goes beyond the Directive in terms of substantive provisions by harmonising rules for requests to remove terrorist content as well as proactive measures.

The proposed Regulation builds upon the Commission's Recommendation[3] on illegal content of March 2018. The Recommendation remains in force, and all those who have a role to play in reducing accessibility to illegal content – including terrorist content - should continue to align their efforts with the measures identified within the Recommendation.

[3] Recommendation (C(2018)1177 final) of 1 March 2018 on measures to effectively tackle illegal content online.

www.parlament.gv.at

1.3. Summary of the proposed Regulation

The personal scope of the proposal includes hosting service providers who offer their services within the Union, regardless of their place of establishment or their size. The proposed legislation introduces a number of measures to prevent the misuse of hosting services for the dissemination of terrorist content online in order to guarantee the smooth functioning of the Digital Single Market, whilst ensuring trust and security. The definition of illegal terrorist content is in accordance with the definition of terrorist offences as set out in Directive (EU) 2017/541 and is defined as information which is used to incite and glorify the commission of terrorist offences, encouraging the contribution to and providing instructions for committing terrorist offences as well as promoting participation in terrorist groups.

To ensure the removal of illegal terrorist content, the Regulation introduces a removal order which can be issued as an administrative or judicial decision by a competent authority in a Member State. In such cases, the hosting service provider is obliged to remove the content or disable access to it within one hour. In addition, the Regulation harmonises the minimum requirements for referrals sent by Member States' competent authorities and by Union bodies (such as Europol) to hosting service providers to be assessed against their respective terms and conditions. Finally, the Regulation requires hosting service providers, where appropriate, to take proactive measures proportionate to the level of risk and to remove terrorist material from their services, including by deploying automated detection tools.

The measures designed to reduce terrorist content online are accompanied by a number of key safeguards to ensure the full protection of fundamental rights. As part of the measures to protect content which is not terrorist content from erroneous removal, the proposal sets out obligations to put in place remedies and complaint mechanisms to ensure that users can challenge the removal of their content. In addition, the Regulation introduces obligations on transparency for the measures taken against terrorist content by hosting service providers, thereby ensuring accountability towards users, citizens and public authorities.

The Regulation also obliges Member States to ensure that their competent authorities have the necessary capacity to intervene against terrorist content online. In addition, Member States are obliged to inform and cooperate with each other and may make use of channels set up by Europol to ensure co-ordination with regards to removal orders and referrals. The regulation also foresees obligations on hosting service providers to report in more detail on the measures taken and inform law enforcement when they detect content which poses a threat to life or safety. Finally, there is an obligation on hosting service providers to preserve the content they remove, which functions as a safeguard against erroneous removal and ensures potential evidence is not lost for the purpose of the prevention, detection, investigation and prosecution of terrorist offences.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

2.1. Legal basis

The legal basis is Article 114 of the Treaty on the Functioning of the European Union, which provides for the establishment of measures to ensure the functioning of the Internal Market.

Article 114 is the appropriate legal basis to harmonise the conditions for hosting service providers to provide services across borders in the Digital Single Market and to address differences between Member State provisions which might otherwise obstruct the functioning

www.parlament.gv.at

of the internal market. It also prevents the emergence of future obstacles to economic activity resulting from differences in the way national laws might develop.

Article 114 TFEU can also be used to impose obligations on services providers established outside the territory of the EU where their service provision affects the internal market, since this is necessary for the desired internal market goal pursued.

2.2. Choice of the instrument

Article 114 TFEU gives the Union's legislator the possibility to adopt regulations and directives.

As the proposal concerns obligations on service providers usually offering their services in more than one Member State, divergence in the application of these rules would hinder the provision of services by providers operating in multiple Member States. A regulation allows for the same obligation to be imposed in a uniform manner across the Union, is directly applicable, provides clarity and greater legal certainty and avoids divergent transposition in the Member States. For these reasons the most appropriate form to be used for this instrument is considered to be a regulation.

2.3. Subsidiarity

Given the cross-border dimension of the problems addressed, the measures included in the proposal need to be adopted at Union level in order to achieve the objectives. The internet is by its nature cross-border, and content hosted in one Member State can normally be accessed from any other Member State.

A fragmented framework of national rules to tackle terrorist content online is appearing and risks increasing. This would result in a burden for companies to comply with diverging regulations and create unequal conditions for companies as well as security loopholes.

EU action therefore enhances legal certainty and increases the effectiveness of hosting service providers' actions against terrorist content online. This should allow more companies to take action, including companies established outside the European Union, strengthening the integrity of the digital single market.

This justifies the need for EU action, as echoed by the European Council Conclusions of June 2018 inviting the Commission to present a legislative proposal in this area.

2.4. Proportionality

The proposal lays down rules for hosting service providers to apply measures to expeditiously remove terrorist content from their services. Key features limit the proposal to only that which is necessary to achieve the policy objectives.

The proposal takes into account the burden on hosting service providers and safeguards, including the protection of freedom of expression and information as well as other fundamental rights. The one-hour timeframe for removal only applies to removal orders, for which competent authorities have determined illegality in a decision which is subject to judicial review. For referrals, there is an obligation to put in place measures to facilitate the expeditious assessment of terrorist content, without however imposing obligations to remove

www.parlament.gv.at

it, nor within absolute deadlines. The final decision remains a voluntary decision by the hosting service provider. The burden on companies to assess the content is alleviated by the fact that the competent authorities of Member States and Union bodies provide explanations why the content may be considered terrorist content. Hosting service providers shall, where appropriate, take proactive measures to protect their services against the dissemination of terrorist content. Specific obligations related to proactive measures are limited to those hosting service providers exposed to terrorist content, as evidenced by the receipt of a removal order which has become final, and should be proportionate to the level of risk as well as resources of the company. The preservation of the removed content and related data is limited for a period of time proportionate to the purposes of enabling proceedings of administrative or judicial review and for the prevention, detection, investigation and prosecution of terrorist offences.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENT

3.1. Stakeholder consultations

In preparing this legislative proposal, the Commission consulted all relevant stakeholders to understand their views and a potential way forward. The Commission conducted an open public consultation on measures to improve the effectiveness of tackling illegal content, receiving 8,961 replies, of which 8,749 were from individuals, 172 from organisations, 10 from public administrations, and 30 from other categories of respondents. In parallel, a Eurobarometer survey was conducted with a random sample of 33,500 EU residents on illegal content online. The Commission also consulted Member States' authorities as well as hosting service providers throughout May and June 2018 with regards to specific measures to tackle terrorist content online.

By and large, most stakeholders expressed that terrorist content online is a serious societal problem affecting internet users and business models of hosting service providers. More generally, 65% of respondent to the Eurobarometer[4] survey considered that the internet is not safe for its users and 90% of the respondents consider it important to limit the spread of illegal content online. Consultations with Member States revealed that while voluntary arrangements are producing results, many see the need for binding obligations on terrorist content, a sentiment echoed in the European Council Conclusions of June 2018. While overall, the hosting service providers were in favour of the continuation of voluntary measures, they noted the potential negative effects of emerging legal fragmentation in the Union.

Many stakeholders also noted the need to ensure that any regulatory measures for removal of content, particularly proactive measures and strict timeframes, should be balanced with safeguards for fundamental rights, notably freedom of speech. Stakeholders noted a number of necessary measures relating to transparency, accountability as well as the need for human review in deploying automated tools.

[4] Eurobarometer 469, Illegal content online, June 2018.

www.parlament.gv.at

3.2. Impact Assessment

The Regulatory Scrutiny Board issued a positive opinion on the impact assessment with reservations and made various suggestions for improvement[5]. Following this opinion, the Impact Assessment report was amended to address the main comments of the Board, setting the focus specifically on terrorist content while further emphasising the implications on the functioning of the Digital Single Market as well as providing a more in depth analysis of the impact on fundamental rights and the functioning of the safeguards proposed in the options.

If no additional measures were taken, voluntary actions under the baseline would be expected to continue and have some impact on reducing terrorist content online. However, voluntary measures are unlikely to be taken by all hosting service providers exposed to such content, and further legal fragmentation is expected to emerge introducing additional barriers to cross-border service provision. Three main policy options were considered besides the baseline scenario with increasing levels of effectiveness in addressing the objectives set out in the impact assessment and the overall policy goal of reducing terrorist content online.

The scope of these obligations in all three options focused on all hosting service providers (personal scope) established in the EU and in third countries - insofar as they offer their services in the Union (geographic scope). Given the nature of the problem and the need to avoid the abuse of smaller platforms, no exemptions are foreseen for SMEs under any of the options. All options would require hosting service providers to establish a legal representative in the EU – including for companies established outside the EU – so as to ensure enforceability of EU rules. Under all options, Member States were foreseen to develop sanction mechanisms.

All options envisaged the creation of a new, harmonised system of legal removal orders relating to terrorist content online, issued by national authorities to hosting service providers and the requirement to remove that content within one hour. These orders would not necessarily require an assessment on the part of the hosting service providers, and would be subject to judicial redress.

Safeguards, notably complaint procedures and effective remedies, including judicial redress as well as other provisions to prevent the erroneous removal of content which is not terrorist content, whilst ensuring compliance with fundamental rights, are all common features of the three options. Furthermore, all options include reporting obligations in the form of public transparency and reporting to Member States and the Commission, as well as towards authorities for suspected criminal offences. In addition, cooperation obligations between national authorities, hosting service providers, and where relevant Europol are foreseen.

The main differences between the three options relate to the scope of the definition of terrorist content, the level of harmonisation of referrals, the scope of proactive measures, co-ordination obligations on Member States, as well as data preservation requirements. Option 1 would limit the material scope to content disseminated to directly incite to commit a terrorist act, following a narrow definition, while options 2 and 3 would adopt a more comprehensive approach, covering also material concerning recruitment and training. On proactive measures, under option 1, hosting service providers exposed to terrorist content would need to carry out a risk assessment but proactive measures addressing the risk would remain voluntary. Option 2 would require hosting service providers to prepare an action plan which may include

[5] Link to the RSB opinion on RegDoc.

www.parlament.gv.at

deploying automated tools for the prevention of re-upload of already removed content. Option 3 includes more comprehensive proactive measures requiring service providers exposed to terrorist content to also identify new material. In all options, the requirements related to proactive measures would be proportionate to the level of exposure to terrorist material as well as the economic capacities of the service provider. With regards to referrals, option 1 would not harmonise the approach to referrals whereas option 2 would do so for Europol and option 3 would additionally include Member States referrals. Under options 2 and 3, Member States would be obliged to inform, coordinate and cooperate with each other and in option 3 they would also have to ensure that their competent authorities have the capacity to detect and notify terrorist content. Finally, option 3 also includes a requirement to preserve data as a safeguard in cases of erroneous removal and to facilitate criminal investigations.

In addition to the legal provisions, all legislative options were envisaged to be accompanied by a series of supporting measures, in particular to facilitate cooperation across national authorities and Europol, as well as the collaboration with hosting service providers, and Research, Development and Innovation support for development and take-up of technological solutions. Additional awareness-raising and supporting instruments for SMEs could also be deployed following the adoption of the legal instrument.

The Impact Assessment concluded that a series of measures are required to achieve the policy objective. The comprehensive definition of terrorist content capturing the most harmful material would be preferable to a narrow definition of content (option 1). Proactive obligations limited to preventing the re-upload of terrorist content (option 2) would be less impactful compared to obligations related to the detection of new terrorist content (option 3). Provisions on referrals should include referrals from both Europol and Member States (option 3) and not be limited to just referrals from Europol (option 2) as referrals from Member States are an important contribution as part of the overall effort on reducing accessibility to terrorist content online. Such measures would need to be implemented in addition to the measures common to all options, including robust safeguards against erroneous removal of content.

3.3. Fundamental rights

Terrorists' online propaganda seeks to incite individuals to carry out terrorist attacks, including by equipping them with detailed instructions on how to inflict maximum harm. Further propaganda is commonly released after such atrocities, whereby they glorify in these acts, and encourage others to follow suit. This Regulation contributes to the protection of public security, by reducing accessibility to terrorist content that promotes and encourages the violation of fundamental rights.

The proposal could potentially affect a number of fundamental rights:

(a) rights of the content provider: right to freedom of expression; right to protection of personal data; right to respect of private and family life, the principle of non-discrimination and the right to an effective remedy;

(b) rights of the service provider: right to freedom to conduct a business; right to an effective remedy;

(c) rights of all citizens: and right to freedom of expression and information.

Taking into account the relevant acquis, appropriate and robust safeguards are included in the proposed Regulation to ensure that the rights of these persons are protected.

www.parlament.gv.at

A first element in this context is that the Regulation establishes a definition of terrorist content online in accordance with the definition of terrorist offences in Directive (EU) 2017/541. This definition applies to removal orders and referrals, as well as to proactive measures. This definition ensures that only illegal content which corresponds to a Union-wide definition of related criminal offences is to be removed. In addition, the Regulation includes general duties of care for hosting services providers to act in a diligent, proportionate and non-discriminatory manner in respect of content that they store, in particular when implementing their own terms and conditions with a view to avoiding removal of content which is not terrorist content.

More specifically, the Regulation has been designed to ensure proportionality of the measures taken with respect to fundamental rights. Regarding removal orders, the assessment of the content (including legal checks, where necessary) by a competent authority justifies the one-hour removal time limit for this measure. Furthermore, the provisions in this Regulation that relate to referrals are limited to those sent by competent authorities and Union bodies providing explanations why the content may be considered terrorist content. While the responsibility for removing content identified in a referral remains with the hosting service provider, this decision is facilitated by the aforementioned assessment.

For proactive measures, the responsibility for identifying, assessing and removing content remains with the hosting service providers and they are required to put in place safeguards to ensure content is not removed erroneously, including through human review, particularly if further contextualisation is required. Furthermore, unlike in the baseline scenario where the most affected companies set up automated tools without public oversight, the design of the measures as well as their implementation would be subject to reporting to competent bodies in Member States. This obligation reduces the risks of erroneous removals both for companies setting up new tools as well as for those who are already using them. In addition, hosting service providers are required to provide user-friendly complaint mechanisms for content providers to contest the decision to remove their content as well as publish transparency reports to the general public.

Finally, should any content and related data be removed erroneously despite these safeguards, hosting service providers are required to preserve it for a period of six months to be able to reinstate it to ensure the effectiveness of complaint and review procedures in view of protecting freedom of expression and information. At the same time, the preservation also contributes to law enforcement purposes. Hosting service providers need to put in place technical and organisational safeguards to ensure the data is not used for other purposes.

The proposed measures, in particular those related to removal orders, referrals, proactive measures and the preservation of data should not only protect internet users against terrorist content but also contribute to protecting the right of citizens to life by reducing the accessibility of terrorist content online.

4. BUDGETARY IMPLICATIONS

The legislative proposal for a Regulation does not have an impact on the Union’s budget.

www.parlament.gv.at

5. OTHER ELEMENTS

5.1. Implementation plans and monitoring, evaluation and reporting arrangements

The Commission will establish within [one year from the date of application of this Regulation] a detailed programme for monitoring the outputs, results and impacts of this Regulation. The monitoring programme shall set out the indicators and the means by which and the intervals at which the data and other necessary evidence will be collected. It shall specify the actions to be taken by the Commission and by the Member States in collecting and analysing the data and other evidence to monitor the progress and evaluate this Regulation.

On the basis of the established monitoring programme, within two years of the entry into force of this Regulation, the Commission will report on the implementation of this Regulation based on the transparency reports published by companies as well as information provided by Member States. The Commission will carry out an evaluation no sooner than four years after the Regulation entered into force.

Based on the findings of the evaluation, including whether certain gaps or vulnerabilities remain, and taking into account technological developments, the Commission will assess the need to enlarge the scope of the Regulation. If necessary, the Commission will submit proposals to adapt this Regulation.

The Commission will support the implementation, monitoring and evaluation of the Regulation through a Commission expert group. The group will also facilitate the cooperation between hosting service providers, law enforcement and Europol; foster exchanges and practices to detect and remove terrorist content, provide its expertise on the evolution of terrorists' modus operandi online; as well as provide advice and guidance where appropriate to allow for the implementation of the provisions.

The implementation of the proposed Regulation could be facilitated through a number of supporting measures. These include the possible development of a platform within Europol to assist in the co-ordination of referrals and removal orders. EU funded research about how terrorists' modus operandi is evolving enhances the understanding and awareness of all relevant stakeholders. In addition, Horizon 2020 supports research with a view to developing new technologies, including automated prevention of uploading of terrorism content. Furthermore, the Commission will continue analysing how to support competent authorities and hosting service providers in the implementation of this Regulation through EU financial instruments.

5.2. Detailed explanation of the specific provisions of the proposal

Article 1 sets out the subject matter, indicating that the Regulation lays down rules to prevent the misuse of hosting services for the dissemination of terrorist content online, including duties of care on hosting service providers and measures to be put in place by Member States. It also sets out the geographical scope, covering hosting service providers offering services in the Union, irrespective of their place of establishment.

Article 2 provides definitions of terms used in the proposal. It also establishes a definition of terrorist content for preventative purposes drawing on the Directive on Combating Terrorism to capture material and information that incites, encourages or advocates the commission or contribution to terrorist offences, provides instructions for the commission of such offences or promotes the participation in activities of a terrorist group.

www.parlament.gv.at

Article 3 provides for duties of care to be applied by hosting service providers when taking action in accordance with this Regulation and in particular, with due regard to the fundamental rights involved. It provides for appropriate provisions to be put in place within hosting service providers' terms and conditions and to then ensure that these are applied.

Article 4 requires Member States to empower competent authorities to issue removal orders and lays down a requirement for hosting service providers to remove content within one hour of the receipt of a removal order. It also sets out the minimum elements removal orders should contain and procedures for hosting service providers to give feedback to the issuing authority, and to inform the latter if it is not possible to comply with the order or if further clarification is required. It also requires the issuing authority to inform the authority overseeing proactive measures of the Member State of jurisdiction of the hosting service provider.

Article 5 lays down a requirement for hosting service providers to put in place measures to expeditiously assess content referred through a referral from either a competent authority in a Member State or a Union body without however imposing a requirement to remove the content referred nor does it set specific deadlines for action. It also sets out the minimum elements referrals should contain and procedures for hosting service providers to give feedback to the issuing authority and to request clarification to the authority which referred the content.

Article 6 requires hosting service providers to take effective and proportionate proactive measures where appropriate. It sets out a procedure ensuring that certain hosting service providers (i.e. those having received a removal order that has become final) take additional proactive measures where necessary to mitigate the risks and in accordance with the exposure of terrorist content on their services. The hosting service provider should cooperate with the competent authority with regards to the necessary measures required, and, if no agreement can be reached, the authority may impose measures upon the service provider. The Article also sets a review procedure of the authority’s decision.

Article 7 requires hosting service providers to preserve removed content and related data for six months for review proceedings and for investigative purposes. This period can be extended in order to allow the finalisation of the review. The Article also requires service providers to put in place safeguards to ensure the preserved content and related data is not accessed or processed for other purposes.

Article 8 lays down an obligation for hosting service providers to explain their policies against terrorist content and to publish annual transparency reports on the actions taken in this regard.

Article 9 provides for specific safeguards regarding the use and implementation of proactive measures when using automated tools to ensure that decisions are accurate and well-founded.

Article 10 requires hosting service providers to implement complaint mechanisms for removals, referrals and proactive measures and to examine promptly every complaint.

Article 11 establishes an obligation for hosting service providers to make available information about the removal to the content provider, unless the competent authority requires the non-disclosure for public security reasons.

www.parlament.gv.at

Article 12 requires Member States to ensure that competent authorities have sufficient capability and resources in order to fulfil their responsibilities under this Regulation.

Article 13 requires Member States to cooperate with each other and where appropriate with Europol to avoid duplication and interference with investigations. The Article also provides for the possibility of Member States and hosting service providers to make use of dedicated tools, including those of Europol, for the processing and feedback of removal orders and referrals and to cooperate on proactive measures. It also requires Member States to have the appropriate communication channels in place to ensure the timely exchange of information in implementing and enforcing provisions under this Regulation. The Article also obliges hosting service providers to inform the relevant authorities when they are aware of any evidence of terrorist offences within the meaning of Article 3 of the Directive (EU) 2017/541 on Combating Terrorism.

Article 14 provides for the establishment of points of contact by both hosting service providers and Member States to facilitate communication between them, particularly in relation to referrals and removal orders.

Article 15 establishes the Member State jurisdiction for the purposes of overseeing proactive measures, setting penalties and monitoring efforts.

Article 16 requires hosting service providers which do not have an establishment within any Member State but which do offer services within the Union, to designate a legal representative in the Union.

Article 17 requires Member States to designate authorities for issuing removal orders, for referring terrorist content, for overseeing the implementation of proactive measures and for enforcement of the Regulation.

Article 18 sets out that Member States should lay down rules on penalties for non-compliance and provides criteria for Member States to take into account when determining the type and level of penalties. Given the particular importance of expeditious removal of terrorist content identified in a removal order, specific rules should be put in place on financial penalties for systematic breaches of this requirement.

Article 19 lays down a faster and more flexible procedure for amending the templates provided for removal orders and authenticated submission channels through delegated acts.

Article 20 lays down the conditions under which the Commission has the power to adopt delegated acts to provide for necessary amendments to the templates and technical requirements for removal orders.

Article 21 requires the Member States to collect and report specific information related to the application of the Regulation with a view to assist the Commission in the exercise of its duties under Article 23. The Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Regulation.

Article 22 sets out that the Commission shall report on the implementation of this Regulation two years after its entry into force.

Article 23 sets out that the Commission shall report on the evaluation of this Regulation no sooner than three years after its entry into force.

www.parlament.gv.at

Article 24 establishes that the proposed Regulation will enter into force the twentieth day after its publication in the Official Journal and will then apply 6 months after its date of entry into force. This deadline is proposed considering the need for implementing measures while also recognising the urgency for full application of the rules of the proposed Regulation. This deadline of 6 months has been set on the assumption that negotiations will be conducted swiftly.

www.parlament.gv.at

2018/0331 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on preventing the dissemination of terrorist content online

A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[6],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) This Regulation aims at ensuring the smooth functioning of the digital single market in an open and democratic society, by preventing the misuse of hosting services for terrorist purposes. The functioning of the digital single market should be improved by reinforcing legal certainty for hosting service providers, reinforcing users' trust in the online environment, and by strengthening safeguards to the freedom of expression and information.

(2) Hosting service providers active on the internet play an essential role in the digital economy by connecting business and citizens and by facilitating public debate and the distribution and receipt of information, opinions and ideas, contributing significantly to innovation, economic growth and job creation in the Union. However, their services are in certain cases abused by third parties to carry out illegal activities online. Of particular concern is the misuse of hosting service providers by terrorist groups and their supporters to disseminate terrorist content online in order to spread their message, to radicalise and recruit and to facilitate and direct terrorist activity.

[6] OJ C , , p. .

www.parlament.gv.at

(3) The presence of terrorist content online has serious negative consequences for users, for citizens and society at large as well as for the online service providers hosting such content, since it undermines the trust of their users and damages their business models. In light of their central role and the technological means and capabilities associated with the services they provide, online service providers have particular societal responsibilities to protect their services from misuse by terrorists and to help tackle terrorist content disseminated through their services.

(4) Efforts at Union level to counter terrorist content online commenced in 2015 through a framework of voluntary cooperation between Member States and hosting service providers need to be complemented by a clear legislative framework in order to further reduce accessibility to terrorist content online and adequately address a rapidly evolving problem. This legislative framework seeks to build on voluntary efforts, which were reinforced by the Commission Recommendation (EU) 2018/334[7] and responds to calls made by the European Parliament to strengthen measures to tackle illegal and harmful content and by the European Council to improve the automatic detection and removal of content that incites to terrorist acts.

(5) The application of this Regulation should not affect the application of Article 14 of Directive 2000/31/EC[8]. In particular, any measures taken by the hosting service provider in compliance with this Regulation, including any proactive measures, should not in themselves lead to that service provider losing the benefit of the liability exemption provided for in that provision. This Regulation leaves unaffected the powers of national authorities and courts to establish liability of hosting service providers in specific cases where the conditions under Article 14 of Directive 2000/31/EC for liability exemption are not met.

(6) Rules to prevent the misuse of hosting services for the dissemination of terrorist content online in order to guarantee the smooth functioning of the internal market are set out in this Regulation in full respect of the fundamental rights protected in the Union's legal order and notably those guaranteed in the Charter of Fundamental Rights of the European Union.

(7) This Regulation contributes to the protection of public security while establishing appropriate and robust safeguards to ensure protection of the fundamental rights at stake. This includes the rights to respect for private life and to the protection of personal data, the right to effective judicial protection, the right to freedom of expression, including the freedom to receive and impart information, the freedom to conduct a business, and the principle of non-discrimination. Competent authorities and hosting service providers should only adopt measures which are necessary, appropriate and proportionate within a democratic society, taking into account the particular importance accorded to the freedom of expression and information, which constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which the Union is founded. Measures constituting interference in the freedom of expression and information should be strictly targeted, in the sense that

---

7 Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online (OJ L 63, 6.3.2018, p. 50).

8 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

www.parlament.gv.at

they must serve to prevent the dissemination of terrorist content, but without thereby affecting the right to lawfully receive and impart information, taking into account the central role of hosting service providers in facilitating public debate and the distribution and receipt of facts, opinions and ideas in accordance with the law.

(8) The right to an effective remedy is enshrined in Article 19 TEU and Article 47 of the Charter of Fundamental Rights of the European Union. Each natural or legal person has the right to an effective judicial remedy before the competent national court against any of the measures taken pursuant to this Regulation, which can adversely affect the rights of that person. The right includes, in particular the possibility for hosting service providers and content providers to effectively contest the removal orders before the court of the Member State whose authorities issued the removal order.

(9) In order to provide clarity about the actions that both hosting service providers and competent authorities should take to prevent the dissemination of terrorist content online, this Regulation should establish a definition of terrorist content for preventative purposes drawing on the definition of terrorist offences under Directive (EU) 2017/541 of the European Parliament and of the Council[9]. Given the need to address the most harmful terrorist propaganda online, the definition should capture material and information that incites, encourages or advocates the commission or contribution to terrorist offences, provides instructions for the commission of such offences or promotes the participation in activities of a terrorist group. Such information includes in particular text, images, sound recordings and videos. When assessing whether content constitutes terrorist content within the meaning of this Regulation, competent authorities as well as hosting service providers should take into account factors such as the nature and wording of the statements, the context in which the statements were made and their potential to lead to harmful consequences, thereby affecting the security and safety of persons. The fact that the material was produced by, is attributable to or disseminated on behalf of an EU-listed terrorist organisation or person constitutes an important factor in the assessment. Content disseminated for educational, journalistic or research purposes should be adequately protected. Furthermore, the expression of radical, polemic or controversial views in the public debate on sensitive political questions should not be considered terrorist content.

(10) In order to cover those online hosting services where terrorist content is disseminated, this Regulation should apply to information society services which store information provided by a recipient of the service at his or her request and in making the information stored available to third parties, irrespective of whether this activity is of a mere technical, automatic and passive nature. By way of example such providers of information society services include social media platforms, video streaming services, video, image and audio sharing services, file sharing and other cloud services to the extent they make the information available to third parties and websites where users can make comments or post reviews. The Regulation should also apply to hosting service providers established outside the Union but offering services within the Union, since a significant proportion of hosting service providers exposed to terrorist content

[9] 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 (OJ L 88, 31.3.2017, p. 6).

www.parlament.gv.at

on their services are established in third countries. This should ensure that all companies operating in the Digital Single Market comply with the same requirements, irrespective of their country of establishment. The determination as to whether a service provider offers services in the Union requires an assessment whether the service provider enables legal or natural persons in one or more Member States to use its services. However, the mere accessibility of a service provider's website or of an email address and of other contact details in one or more Member States taken in isolation should not be a sufficient condition for the application of this Regulation.

(11) A substantial connection to the Union should be relevant to determine the scope of this Regulation. Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union or, in its absence, on the basis of the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States can be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services. The targeting of activities towards a Member State could also be derived from the availability of an application in the relevant national application store, from providing local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State. A substantial connection should also be assumed where a service provider directs its activities towards one or more Member State as set out in Article 17(1)(c) of Regulation 1215/2012 of the European Parliament and of the Council[10]. On the other hand, provision of the service in view of mere compliance with the prohibition to discriminate laid down in Regulation (EU) 2018/302 of the European Parliament and of the Council[11] cannot, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union.

(12) Hosting service providers should apply certain duties of care, in order to prevent the dissemination of terrorist content on their services. These duties of care should not amount to a general monitoring obligation. Duties of care should include that, when applying this Regulation, hosting services providers act in a diligent, proportionate and non-discriminatory manner in respect of content that they store, in particular when implementing their own terms and conditions, with a view to avoiding removal of content which is not terrorist. The removal or disabling of access has to be undertaken in the observance of freedom of expression and information.

(13) The procedure and obligations resulting from legal orders requesting hosting service providers to remove terrorist content or disable access to it, following an assessment by the competent authorities, should be harmonised. Member States should remain free as to the choice of the competent authorities allowing them to designate administrative, law enforcement or judicial authorities with that task. Given the speed

[10] Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

[11] Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC (OJ L 601, 2.3.2018, p. 1).

www.parlament.gv.at

at which terrorist content is disseminated across online services, this provision imposes obligations on hosting service providers to ensure that terrorist content identified in the removal order is removed or access to it is disabled within one hour from receiving the removal order. It is for the hosting service providers to decide whether to remove the content in question or disable access to the content for users in the Union.

(14) The competent authority should transmit the removal order directly to the addressee and point of contact by any electronic means capable of producing a written record under conditions that allow the service provider to establish authenticity, including the accuracy of the date and the time of sending and receipt of the order, such as by secured email and platforms or other secured channels, including those made available by the service provider, in line with the rules protecting personal data. This requirement may notably be met by the use of qualified electronic registered delivery services as provided for by Regulation (EU) 910/2014 of the European Parliament and of the Council[12].

(15) Referrals by the competent authorities or Europol constitute an effective and swift means of making hosting service providers aware of specific content on their services. This mechanism of alerting hosting service providers to information that may be considered terrorist content, for the provider's voluntary consideration of the compatibility its own terms and conditions, should remain available in addition to removal orders. It is important that hosting service providers assess such referrals as a matter of priority and provide swift feedback about action taken. The ultimate decision about whether or not to remove the content because it is not compatible with their terms and conditions remains with the hosting service provider. In implementing this Regulation related to referrals, Europol's mandate as laid down in Regulation (EU) 2016/794[13] remains unaffected.

(16) Given the scale and speed necessary for effectively identifying and removing terrorist content, proportionate proactive measures, including by using automated means in certain cases, are an essential element in tackling terrorist content online. With a view to reducing the accessibility of terrorist content on their services, hosting service providers should assess whether it is appropriate to take proactive measures depending on the risks and level of exposure to terrorist content as well as to the effects on the rights of third parties and the public interest of information. Consequently, hosting service providers should determine what appropriate, effective and proportionate proactive measure should be put in place. This requirement should not imply a general monitoring obligation. In the context of this assessment, the absence of removal orders and referrals addressed to a hosting provider, is an indication of a low level of exposure to terrorist content.

---

12 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

13 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

www.parlament.gv.at

(17) When putting in place proactive measures, hosting service providers should ensure that users' right to freedom of expression and information - including to freely receive and impart information - is preserved. In addition to any requirement laid down in the law, including the legislation on protection of personal data, hosting service providers should act with due diligence and implement safeguards, including notably human oversight and verifications, where appropriate, to avoid any unintended and erroneous decision leading to removal of content that is not terrorist content. This is of particular relevance when hosting service providers use automated means to detect terrorist content. Any decision to use automated means, whether taken by the hosting service provider itself or pursuant to a request by the competent authority, should be assessed with regard to the reliability of the underlying technology and the ensuing impact on fundamental rights.

(18) In order to ensure that hosting service providers exposed to terrorist content take appropriate measures to prevent the misuse of their services, the competent authorities should request hosting service providers having received a removal order, which has become final, to report on the proactive measures taken. These could consist of measures to prevent the re-upload of terrorist content, removed or access to it disabled as a result of a removal order or referrals they received, checking against publicly or privately-held tools containing known terrorist content. They may also employ the use of reliable technical tools to identify new terrorist content, either using those available on the market or those developed by the hosting service provider. The service provider should report on the specific proactive measures in place in order to allow the competent authority to judge whether the measures are effective and proportionate and whether, if automated means are used, the hosting service provider has the necessary abilities for human oversight and verification. In assessing the effectiveness and proportionality of the measures, competent authorities should take into account relevant parameters including the number of removal orders and referrals issued to the provider, their economic capacity and the impact of its service in disseminating terrorist content (for example, taking into account the number of users in the Union).

(19) Following the request, the competent authority should enter into a dialogue with the hosting service provider about the necessary proactive measures to be put in place. If necessary, the competent authority should impose the adoption of appropriate, effective and proportionate proactive measures where it considers that the measures taken are insufficient to meet the risks. A decision to impose such specific proactive measures should not, in principle, lead to the imposition of a general obligation to monitor, as provided in Article 15(1) of Directive 2000/31/EC. Considering the particularly grave risks associated with the dissemination of terrorist content, the decisions adopted by the competent authorities on the basis of this Regulation could derogate from the approach established in Article 15(1) of Directive 2000/31/EC, as regards certain specific, targeted measures, the adoption of which is necessary for overriding public security reasons. Before adopting such decisions, the competent authority should strike a fair balance between the public interest objectives and the fundamental rights involved, in particular, the freedom of expression and information and the freedom to conduct a business, and provide appropriate justification.

(20) The obligation on hosting service providers to preserve removed content and related data, should be laid down for specific purposes and limited in time to what is necessary. There is need to extend the preservation requirement to related data to the extent that any such data would otherwise be lost as a consequence of the removal of

www.parlament.gv.at

the content in question. Related data can include data such as ‘subscriber data’, including in particular data pertaining to the identity of the content provider as well as ‘access data’, including for instance data about the date and time of use by the content provider, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the content provider.

(21) The obligation to preserve the content for proceedings of administrative or judicial review is necessary and justified in view of ensuring the effective measures of redress for the content provider whose content was removed or access to it disabled as well as for ensuring the reinstatement of that content as it was prior to its removal depending on the outcome of the review procedure. The obligation to preserve content for investigative and prosecutorial purposes is justified and necessary in view of the value this material could bring for the purpose of disrupting or preventing terrorist activity. Where companies remove material or disable access to it, in particular through their own proactive measures, and do not inform the relevant authority because they assess that it does not fall in the scope of Article 13(4) of this Regulation, law enforcement may be unaware of the existence of the content. Therefore, the preservation of content for purposes of prevention, detection, investigation and prosecution of terrorist offences is also justified. For these purposes, the required preservation of data is limited to data that is likely to have a link with terrorist offences, and can therefore contribute to prosecuting terrorist offences or to preventing serious risks to public security.

(22) To ensure proportionality, the period of preservation should be limited to six months to allow the content providers sufficient time to initiate the review process and to enable law enforcement access to relevant data for the investigation and prosecution of terrorist offences. However, this period may be prolonged for the period that is necessary in case the review proceedings are initiated but not finalised within the six months period upon request by the authority carrying out the review. This duration should be sufficient to allow law enforcement authorities to preserve the necessary evidence in relation to investigations, while ensuring the balance with the fundamental rights concerned.

(23) This Regulation does not affect the procedural guarantees and procedural investigation measures related to the access to content and related data preserved for the purposes of the investigation and prosecution of terrorist offences, as regulated under the national law of the Member States, and under Union legislation.

(24) Transparency of hosting service providers' policies in relation to terrorist content is essential to enhance their accountability towards their users and to reinforce trust of citizens in the Digital Single Market. Hosting service providers should publish annual transparency reports containing meaningful information about action taken in relation to the detection, identification and removal of terrorist content.

(25) Complaint procedures constitute a necessary safeguard against erroneous removal of content protected under the freedom of expression and information. Hosting service providers should therefore establish user-friendly complaint mechanisms and ensure that complaints are dealt with promptly and in full transparency towards the content provider. The requirement for the hosting service provider to reinstate the content where it has been removed in error, does not affect the possibility of hosting service providers to enforce their own terms and conditions on other grounds.

www.parlament.gv.at

(26) Effective legal protection according to Article 19 TEU and Article 47 of the Charter of Fundamental Rights of the European Union requires that persons are able to ascertain the reasons upon which the content uploaded by them has been removed or access to it disabled. For that purpose, the hosting service provider should make available to the content provider meaningful information enabling the content provider to contest the decision. However, this does not necessarily require a notification to the content provider. Depending on the circumstances, hosting service providers may replace content which is considered terrorist content, with a message that it has been removed or disabled in accordance with this Regulation. Further information about the reasons as well as possibilities for the content provider to contest the decision should be given upon request. Where competent authorities decide that for reasons of public security including in the context of an investigation, it is considered inappropriate or counter-productive to directly notify the content provider of the removal or disabling of content, they should inform the hosting service provider.

(27) In order to avoid duplication and possible interferences with investigations, the competent authorities should inform, coordinate and cooperate with each other and where appropriate with Europol when issuing removal orders or sending referrals to hosting service providers. In implementing the provisions of this Regulation, Europol could provide support in line with its current mandate and existing legal framework.

(28) In order to ensure the effective and sufficiently coherent implementation of proactive measures, competent authorities in Member States should liaise with each other with regard to the discussions they have with hosting service providers as to the identification, implementation and assessment of specific proactive measures. Similarly, such cooperation is also needed in relation to the adoption of rules on penalties, as well as the implementation and the enforcement of penalties.

(29) It is essential that the competent authority within the Member State responsible for imposing penalties is fully informed about the issuing of removal orders and referrals and subsequent exchanges between the hosting service provider and the relevant competent authority. For that purpose, Member States should ensure appropriate communication channels and mechanisms allowing the sharing of relevant information in a timely manner.

(30) To facilitate the swift exchanges between competent authorities as well as with hosting service providers, and to avoid duplication of effort, Member States may make use of tools developed by Europol, such as the current Internet Referral Management application (IRMa) or successor tools.

(31) Given the particular serious consequences of certain terrorist content, hosting service providers should promptly inform the authorities in the Member State concerned or the competent authorities where they are established or have a legal representative, about the existence of any evidence of terrorist offences that they become aware of. In order to ensure proportionality, this obligation is limited to terrorist offences as defined in Article 3(1) of Directive (EU) 2017/541. The obligation to inform does not imply an obligation on hosting service providers to actively seek any such evidence. The Member State concerned is the Member State which has jurisdiction over the investigation and prosecution of the terrorist offences pursuant to Directive (EU) 2017/541 based on the nationality of the offender or of the potential victim of the offence or the target location of the terrorist act. In case of doubt, hosting service

www.parlament.gv.at

providers may transmit the information to Europol which should follow up according to its mandate, including forwarding to the relevant national authorities.

(32) The competent authorities in the Member States should be allowed to use such information to take investigatory measures available under Member State or Union law, including issuing a European Production Order under Regulation on European Production and Preservation Orders for electronic evidence in criminal matters[14].

(33) Both hosting service providers and Member States should establish points of contact to facilitate the swift handling of removal orders and referrals. In contrast to the legal representative, the point of contact serves operational purposes. The hosting service provider's point of contact should consist of any dedicated means allowing for the electronic submission of removal orders and referrals and of technical and personal means allowing for the swift processing thereof. The point of contact for the hosting service provider does not have to be located in the Union and the hosting service provider is free to nominate an existing point of contact, provided that this point of contact is able to fulfil the functions provided for in this Regulation. With a view to ensure that terrorist content is removed or access to it is disabled within one hour from the receipt of a removal order, hosting service providers should ensure that the point of contact is reachable 24/7. The information on the point of contact should include information about the language in which the point of contact can be addressed. In order to facilitate the communication between the hosting service providers and the competent authorities, hosting service providers are encouraged to allow for communication in one of the official languages of the Union in which their terms and conditions are available.

(34) In the absence of a general requirement for service providers to ensure a physical presence within the territory of the Union, there is a need to ensure clarity under which Member State's jurisdiction the hosting service provider offering services within the Union falls. As a general rule, the hosting service provider falls under the jurisdiction of the Member State in which it has its main establishment or in which it has designated a legal representative. Nevertheless, where another Member State issues a removal order, its authorities should be able to enforce their orders by taking coercive measures of a non-punitive nature, such as penalty payments. With regards to a hosting service provider which has no establishment in the Union and does not designate a legal representative, any Member State should, nevertheless, be able to issue penalties, provided that the principle of *ne bis in idem* is respected.

(35) Those hosting service providers which are not established in the Union, should designate in writing a legal representative in order to ensure the compliance with and enforcement of the obligations under this Regulation.

(36) The legal representative should be legally empowered to act on behalf of the hosting service provider.

(37) For the purposes of this Regulation, Member States should designate competent authorities. The requirement to designate competent authorities does not necessarily require the establishment of new authorities but can be existing bodies tasked with the

[14] COM(2018)225 final.

www.parlament.gv.at

functions set out in this Regulation. This Regulation requires designating authorities competent for issuing removal orders, referrals and for overseeing proactive measures and for imposing penalties. It is for Member States to decide how many authorities they wish to designate for these tasks.

(38) Penalties are necessary to ensure the effective implementation by hosting service providers of the obligations pursuant to this Regulation. Member States should adopt rules on penalties, including, where appropriate, fining guidelines. Particularly severe penalties shall be ascertained in the event that the hosting service provider systematically fails to remove terrorist content or disable access to it within one hour from receipt of a removal order. Non-compliance in individual cases could be sanctioned while respecting the principles of *ne bis in idem and of* proportionality and ensuring that such sanctions take account of systematic failure. In order to ensure legal certainty, the regulation should set out to what extent the relevant obligations can be subject to penalties. Penalties for non-compliance with Article 6 should only be adopted in relation to obligations arising from a request to report pursuant to Article 6(2) or a decision imposing additional proactive measures pursuant to Article 6(4). When determining whether or not financial penalties should be imposed, due account should be taken of the financial resources of the provider. Member States shall ensure that penalties do not encourage the removal of content which is not terrorist content.

(39) The use of standardised templates facilitates cooperation and the exchange of information between competent authorities and service providers, allowing them to communicate more quickly and effectively. It is particularly important to ensure swift action following the receipt of a removal order. Templates reduce translation costs and contribute to a high quality standard. Response forms similarly should allow for a standardised exchange of information, and this will be particularly important where service providers are unable to comply. Authenticated submission channels can guarantee the authenticity of the removal order, including the accuracy of the date and the time of sending and receipt of the order.

(40) In order to allow for a swift amendment, where necessary, of the content of the templates to be used for the purposes of this Regulation the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission to amend Annexes I, II and III of this Regulation. In order to be able to take into account the development of technology and of the related legal framework, the Commission should also be empowered to adopt delegated acts to supplement this Regulation with technical requirements for the electronic means to be used by competent authorities for the transmission of removal orders. It is of particular importance that the Commission carries out appropriate consultations during its preparatory work, including at expert level, and that those consultations are conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[15]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

[15] OJ L 123, 12.5.2016, p. 1.

www.parlament.gv.at

(41) Member States should collect information on the implementation of the legislation. A detailed programme for monitoring the outputs, results and impacts of this Regulation should be established in order to inform an evaluation of the legislation.

(42) Based on the findings and conclusions in the implementation report and the outcome of the monitoring exercise, the Commission should carry out an evaluation of this Regulation no sooner than three years after its entry into force. The evaluation should be based on the five criteria of efficiency, effectiveness, relevance, coherence and EU added value. It will assess the functioning of the different operational and technical measures foreseen under the Regulation, including the effectiveness of measures to enhance the detection, identification and removal of terrorist content, the effectiveness of safeguard mechanisms as well as the impacts on potentially affected rights and interests of third parties, including a review of the requirement to inform content providers.

(43) Since the objective of this Regulation, namely ensuring the smooth functioning of the digital single market by preventing the dissemination of terrorist content online, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the limitation, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective,

HAVE ADOPTED THIS REGULATION:

SECTION I
GENERAL PROVISIONS

Article 1
Subject matter and scope

1. This Regulation lays down uniform rules to prevent the misuse of hosting services for the dissemination of terrorist content online. It lays down in particular:

   (a) rules on duties of care to be applied by hosting service providers in order to prevent the dissemination of terrorist content through their services and ensure, where necessary, its swift removal;

   (b) a set of measures to be put in place by Member States to identify terrorist content, to enable its swift removal by hosting service providers and to facilitate cooperation with the competent authorities in other Member States, hosting service providers and where appropriate relevant Union bodies.

2. This Regulation shall apply to hosting service providers offering services in the Union, irrespective of their place of main establishment.

Article 2
Definitions

For the purposes of this Regulation, the following definitions shall apply:

www.parlament.gv.at

(1) 'hosting service provider' means 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 stored available to third parties;

(2) 'content provider' means a user who has provided information that is, or that has been, stored at the request of the user by a hosting service provider;

(3) 'to offer services in the Union' means: enabling legal or natural persons in one or more Member States to use the services of the hosting service provider which has a substantial connection to that Member State or Member States, such as

(a) establishment of the hosting service provider in the Union;

(b) significant number of users in one or more Member States;

(c) targeting of activities towards one or more Member States.

(4) 'terrorist offences' means offences as defined in Article 3(1) of Directive (EU) 2017/541;

(5) 'terrorist content' means one or more of the following information:

(a) inciting or advocating, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed;

(b) encouraging the contribution to terrorist offences;

(c) promoting the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Article 2(3) of Directive (EU) 2017/541;

(d) instructing on methods or techniques for the purpose of committing terrorist offences.

(6) 'dissemination of terrorist content' means making terrorist content available to third parties on the hosting service providers' services;

(7) 'terms and conditions' means all terms, conditions and clauses, irrespective of their name or form, which govern the contractual relationship between the hosting service provider and their users;

(8) 'referral' means a notice by a competent authority or, where applicable, a relevant Union body to a hosting service provider about information that may be considered terrorist content, for the provider's voluntary consideration of the compatibility with its own terms and conditions aimed to prevent dissemination of terrorism content;

(9) 'main establishment' means the head office or registered office within which the principal financial functions and operational control are exercised.

SECTION II

MEASURES TO PREVENT THE DISSEMINATION OF TERRORIST CONTENT ONLINE

www.parlament.gv.at

Article 3
Duties of care

1. Hosting service providers shall take appropriate, reasonable and proportionate actions in accordance with this Regulation, against the dissemination of terrorist content and to protect users from terrorist content. In doing so, they shall act in a diligent, proportionate and non-discriminatory manner, and with due regard to the fundamental rights of the users and take into account the fundamental importance of the freedom of expression and information in an open and democratic society.

2. Hosting service providers shall include in their terms and conditions, and apply, provisions to prevent the dissemination of terrorist content.

Article 4
Removal orders

1. The competent authority shall have the power to issue a decision requiring the hosting service provider to remove terrorist content or disable access to it.

2. Hosting service providers shall remove terrorist content or disable access to it within one hour from receipt of the removal order.

3. Removal orders shall contain the following elements in accordance with the template set out in Annex I:

   (a) identification of the competent authority issuing the removal order and authentication of the removal order by the competent authority;

   (b) a statement of reasons explaining why the content is considered terrorist content, at least, by reference to the categories of terrorist content listed in Article 2(5);

   (c) a Uniform Resource Locator (URL) and, where necessary, additional information enabling the identification of the content referred;

   (d) a reference to this Regulation as the legal basis for the removal order;

   (e) date and time stamp of issuing;

   (f) information about redress available to the hosting service provider and to the content provider;

   (g) where relevant, the decision not to disclose information about the removal of terrorist content or the disabling of access to it referred to in Article 11.

4. Upon request by the hosting service provider or by the content provider, the competent authority shall provide a detailed statement of reasons, without prejudice to the obligation of the hosting service provider to comply with the removal order within the deadline set out in paragraph 2.

5. The competent authorities shall address removal orders to the main establishment of the hosting service provider or to the legal representative designated by the hosting

www.parlament.gv.at

service provider pursuant to Article 16 and transmit it to the point of contact referred to in Article 14(1). Such orders shall be sent by electronic means capable of producing a written record under conditions allowing to establish the authentication of the sender, including the accuracy of the date and the time of sending and receipt of the order.

6. Hosting service providers shall acknowledge receipt and, without undue delay, inform the competent authority about the removal of terrorist content or disabling access to it, indicating, in particular, the time of action, using the template set out in Annex II.

7. If the hosting service provider cannot comply with the removal order because of force majeure or of de facto impossibility not attributable to the hosting service provider, it shall inform, without undue delay, the competent authority, explaining the reasons, using the template set out in Annex III. The deadline set out in paragraph 2 shall apply as soon as the reasons invoked are no longer present.

8. If the hosting service provider cannot comply with the removal order because the removal order contains manifest errors or does not contain sufficient information to execute the order, it shall inform the competent authority without undue delay, asking for the necessary clarification, using the template set out in Annex III. The deadline set out in paragraph 2 shall apply as soon as the clarification is provided.

9. The competent authority which issued the removal order shall inform the competent authority which oversees the implementation of proactive measures, referred to in Article 17(1)(c) when the removal order becomes final. A removal order becomes final where it has not been appealed within the deadline according to the applicable national law or where it has been confirmed following an appeal.

Article 5
Referrals

1. The competent authority or the relevant Union body may send a referral to a hosting service provider.

2. Hosting service providers shall put in place operational and technical measures facilitating the expeditious assessment of content that has been sent by competent authorities and, where applicable, relevant Union bodies for their voluntary consideration.

3. The referral shall be addressed to the main establishment of the hosting service provider or to the legal representative designated by the service provider pursuant to Article 16 and transmitted to the point of contact referred to in Article 14(1). Such referrals shall be sent by electronic means.

4. The referral shall contain sufficiently detailed information, including the reasons why the content is considered terrorist content, a URL and, where necessary, additional information enabling the identification of the terrorist content referred.

www.parlament.gv.at

5. The hosting service provider shall, as a matter of priority, assess the content identified in the referral against its own terms and conditions and decide whether to remove that content or to disable access to it.

6. The hosting service provider shall expeditiously inform the competent authority or relevant Union body of the outcome of the assessment and the timing of any action taken as a result of the referral.

7. Where the hosting service provider considers that the referral does not contain sufficient information to assess the referred content, it shall inform without delay the competent authorities or relevant Union body, setting out what further information or clarification is required.

Article 6
Proactive measures

1. Hosting service providers shall, where appropriate, take proactive measures to protect their services against the dissemination of terrorist content. The measures shall be effective and proportionate, taking into account the risk and level of exposure to terrorist content, the fundamental rights of the users, and the fundamental importance of the freedom of expression and information in an open and democratic society.

2. Where it has been informed according to Article 4(9), the competent authority referred to in Article 17(1)(c) shall request the hosting service provider to submit a report, within three months after receipt of the request and thereafter at least on an annual basis, on the specific proactive measures it has taken, including by using automated tools, with a view to:

   (a) preventing the re-upload of content which has previously been removed or to which access has been disabled because it is considered to be terrorist content;

   (b) detecting, identifying and expeditiously removing or disabling access to terrorist content.

   Such a request shall be sent to the main establishment of the hosting service provider or to the legal representative designated by the service provider.

   The reports shall include all relevant information allowing the competent authority referred to in Article 17(1)(c) to assess whether the proactive measures are effective and proportionate, including to evaluate the functioning of any automated tools used as well as the human oversight and verification mechanisms employed.

3. Where the competent authority referred to in Article 17(1)(c) considers that the proactive measures taken and reported under paragraph 2 are insufficient in mitigating and managing the risk and level of exposure, it may request the hosting service provider to take specific additional proactive measures. For that purpose, the hosting service provider shall cooperate with the competent authority referred to in Article 17(1)(c) with a view to identifying the specific measures that the hosting service provider shall put in place, establishing key objectives and benchmarks as well as timelines for their implementation.

www.parlament.gv.at

4. Where no agreement can be reached within the three months from the request pursuant to paragraph 3, the competent authority referred to in Article 17(1)(c) may issue a decision imposing specific additional necessary and proportionate proactive measures. The decision shall take into account, in particular, the economic capacity of the hosting service provider and the effect of such measures on the fundamental rights of the users and the fundamental importance of the freedom of expression and information. Such a decision shall be sent to the main establishment of the hosting service provider or to the legal representative designated by the service provider. The hosting service provider shall regularly report on the implementation of such measures as specified by the competent authority referred to in Article 17(1)(c).

5. A hosting service provider may, at any time, request the competent authority referred to in Article 17(1)(c) a review and, where appropriate, to revoke a request or decision pursuant to paragraphs 2, 3, and 4 respectively. The competent authority shall provide a reasoned decision within a reasonable period of time after receiving the request by the hosting service provider.

Article 7
Preservation of content and related data

1. Hosting service providers shall preserve terrorist content which has been removed or disabled as a result of a removal order, a referral or as a result of proactive measures pursuant to Articles 4, 5 and 6 and related data removed as a consequence of the removal of the terrorist content and which is necessary for:

   (a) proceedings of administrative or judicial review,

   (b) the prevention, detection, investigation and prosecution of terrorist offences.

2. The terrorist content and related data referred to in paragraph 1 shall be preserved for six months. The terrorist content shall, upon request from the competent authority or court, be preserved for a longer period when and for as long as necessary for ongoing proceedings of administrative or judicial review referred to in paragraph 1(a).

3. Hosting service providers shall ensure that the terrorist content and related data preserved pursuant to paragraphs 1 and 2 are subject to appropriate technical and organisational safeguards.

   Those technical and organisational safeguards shall ensure that the preserved terrorist content and related data is only accessed and processed for the purposes referred to in paragraph 1, and ensure a high level of security of the personal data concerned. Hosting service providers shall review and update those safeguards where necessary.

SECTION III
SAFEGUARDS AND ACCOUNTABILITY

Article 8
Transparency obligations

1. Hosting service providers shall set out in their terms and conditions their policy to prevent the dissemination of terrorist content, including, where appropriate, a

www.parlament.gv.at

meaningful explanation of the functioning of proactive measures including the use of automated tools.

2. Hosting service providers shall publish annual transparency reports on action taken against the dissemination of terrorist content.

3. Transparency reports shall include at least the following information:

(a) information about the hosting service provider's measures in relation to the detection, identification and removal of terrorist content;

(b) information about the hosting service provider's measures to prevent the re-upload of content which has previously been removed or to which access has been disabled because it is considered to be terrorist content;

(c) number of pieces of terrorist content removed or to which access has been disabled, following removal orders, referrals, or proactive measures, respectively;

(d) overview and outcome of complaint procedures.

Article 9

Safeguards regarding the use and implementation of proactive measures

1. Where hosting service providers use automated tools pursuant to this Regulation in respect of content that they store, they shall provide effective and appropriate safeguards to ensure that decisions taken concerning that content, in particular decisions to remove or disable content considered to be terrorist content, are accurate and well-founded.

2. Safeguards shall consist, in particular, of human oversight and verifications where appropriate and, in any event, where a detailed assessment of the relevant context is required in order to determine whether or not the content is to be considered terrorist content.

Article 10

Complaint mechanisms

1. Hosting service providers shall establish effective and accessible mechanisms allowing content providers whose content has been removed or access to it disabled as a result of a referral pursuant to Article 5 or of proactive measures pursuant to Article 6, to submit a complaint against the action of the hosting service provider requesting reinstatement of the content.

2. Hosting service providers shall promptly examine every complaint that they receive and reinstate the content without undue delay where the removal or disabling of access was unjustified. They shall inform the complainant about the outcome of the examination.

www.parlament.gv.at

Article 11
Information to content providers

1. Where hosting service providers removed terrorist content or disable access to it, they shall make available to the content provider information on the removal or disabling of access to terrorist content.

2. Upon request of the content provider, the hosting service provider shall inform the content provider about the reasons for the removal or disabling of access and possibilities to contest the decision.

3. The obligation pursuant to paragraphs 1 and 2 shall not apply where the competent authority decides that there should be no disclosure for reasons of public security, such as the prevention, investigation, detection and prosecution of terrorist offences, for as long as necessary, but not exceeding [four] weeks from that decision. In such a case, the hosting service provider shall not disclose any information on the removal or disabling of access to terrorist content.

SECTION IV
Cooperation between Competent Authorities, Union Bodies and Hosting Service Providers

Article 12
Capabilities of competent authorities

Member States shall ensure that their competent authorities have the necessary capability and sufficient resources to achieve the aims and fulfil their obligations under this Regulation.

Article 13
Cooperation between hosting service providers, competent authorities and where appropriate relevant Union bodies

1. Competent authorities in Member States shall inform, coordinate and cooperate with each other and, where appropriate, with relevant Union bodies such as Europol with regard to removal orders and referrals to avoid duplication, enhance coordination and avoid interference with investigations in different Member States.

2. Competent authorities in Member States shall inform, coordinate and cooperate with the competent authority referred to in Article 17(1)(c) and (d) with regard to measures taken pursuant to Article 6 and enforcement actions pursuant to Article 18. Member States shall make sure that the competent authority referred to in Article 17(1)(c) and (d) is in possession of all the relevant information. For that purpose, Member States shall provide for the appropriate communication channels or mechanisms to ensure that the relevant information is shared in a timely manner.

3. Member States and hosting service providers may choose to make use of dedicated tools, including, where appropriate, those established by relevant Union bodies such as Europol, to facilitate in particular:

   (a) the processing and feedback relating to removal orders pursuant to Article 4;

www.parlament.gv.at

(b) the processing and feedback relating to referrals pursuant to Article 5;

(c) co-operation with a view to identify and implement proactive measures pursuant to Article 6.

4. Where hosting service providers become aware of any evidence of terrorist offences, they shall promptly inform authorities competent for the investigation and prosecution in criminal offences in the concerned Member State or the point of contact in the Member State pursuant to Article 14(2), where they have their main establishment or a legal representative. Hosting service providers may, in case of doubt, transmit this information to Europol for appropriate follow up.

Article 14
Points of contact

1. Hosting service providers shall establish a point of contact allowing for the receipt of removal orders and referrals by electronic means and ensure their swift processing pursuant to Articles 4 and 5. They shall ensure that this information is made publicly available.

2. The information referred to in paragraph 1 shall specify the official language or languages (s) of the Union, as referred to in Regulation 1/58, in which the contact point can be addressed and in which further exchanges in relation to removal orders and referrals pursuant to Articles 4 and 5 shall take place. This shall include at least one of the official languages of the Member State in which the hosting service provider has its main establishment or where its legal representative pursuant to Article 16 resides or is established.

3. Member States shall establish a point of contact to handle requests for clarification and feedback in relation to removal orders and referrals issued by them. Information about the contact point shall be made publicly available.

SECTION V
IMPLEMENTATION AND ENFORCEMENT

Article 15
Jurisdiction

1. The Member State in which the main establishment of the hosting service provider is located shall have the jurisdiction for the purposes of Articles 6, 18, and 21. A hosting service provider which does not have its main establishment within one of the Member States shall be deemed to be under the jurisdiction of the Member State where the legal representative referred to in Article 16 resides or is established.

2. Where a hosting service provider fails to designate a legal representative, all Member States shall have jurisdiction.

3. Where an authority of another Member State has issued a removal order according to Article 4(1), that Member State has jurisdiction to take coercive measures according to its national law in order to enforce the removal order.

www.parlament.gv.at

Article 16
Legal representative

1. A hosting service provider which does not have an establishment in the Union but offers services in the Union, shall designate, in writing, a legal or natural person as its legal representative in the Union for the receipt of, compliance with and enforcement of removal orders, referrals, requests and decisions issued by the competent authorities on the basis of this Regulation. The legal representative shall reside or be established in one of the Member States where the hosting service provider offers the services.

2. The hosting service provider shall entrust the legal representative with the receipt, compliance and enforcement of the removal orders, referrals, requests and decisions referred to in paragraph 1 on behalf of the hosting service provider concerned. Hosting service providers shall provide their legal representative with the necessary powers and resource to cooperate with the competent authorities and comply with these decisions and orders.

3. The designated legal representative can be held liable for non-compliance with obligations under this Regulation, without prejudice to the liability and legal actions that could be initiated against the hosting service provider.

4. The hosting service provider shall notify the competent authority referred to in Article 17(1)(d) in the Member State where the legal representative resides or is established about the designation. Information about the legal representative shall be publicly available.

SECTION VI
FINAL PROVISIONS

Article 17
Designation of competent authorities

1. Each Member State shall designate the authority or authorities competent to

   (a) issue removal orders pursuant to Article 4;

   (b) detect, identify and refer terrorist content to hosting service providers pursuant to Article 5;

   (c) oversee the implementation of proactive measures pursuant to Article 6;

   (d) enforce the obligations under this Regulation through penalties pursuant to Article 18.

2. By [*six months after the entry into force of this Regulation*] at the latest Member States shall notify the Commission of the competent authorities referred to in paragraph 1. The Commission shall publish the notification and any modifications of it in the *Official Journal of the European Union*.

www.parlament.gv.at

Article 18
Penalties

1. Member States shall lay down the rules on penalties applicable to breaches of the obligations by hosting service providers under this Regulation and shall take all necessary measures to ensure that they are implemented. Such penalties shall be limited to infringement of the obligations pursuant to:

   (a) Article 3(2) (hosting service providers' terms and conditions);

   (b) Article 4(2) and (6) (implementation of and feedback on removal orders);

   (c) Article 5(5) and (6) (assessment of and feedback on referrals);

   (d) Article 6(2) and (4) (reports on proactive measures and the adoption of measures following a decision imposing specific proactive measures);

   (e) Article 7 (preservation of data);

   (f) Article 8 (transparency);

   (g) Article 9 (safeguards in relation to proactive measures);

   (h) Article 10 (complaint procedures);

   (i) Article 11 (information to content providers);

   (j) Article 13 (4) (information on evidence of terrorist offences);

   (k) Article 14 (1) (points of contact);

   (l) Article 16 (designation of a legal representative).

2. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by [*within six months from the entry into force of this Regulation*] at the latest, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

3. Member States shall ensure that, when determining the type and level of penalties, the competent authorities take into account all relevant circumstances, including:

   (a) the nature, gravity, and duration of the breach;

   (b) the intentional or negligent character of the breach;

   (c) previous breaches by the legal person held responsible;

   (d) the financial strength of the legal person held liable;

   (e) the level of cooperation of the hosting service provider with the competent authorities.

www.parlament.gv.at

4. Member States shall ensure that a systematic failure to comply with obligations pursuant to Article 4(2) is subject to financial penalties of up to 4% of the hosting service provider's global turnover of the last business year.

Article 19
Technical requirements and amendments to the templates for removal orders

1. The Commission shall be empowered to adopt delegated acts in accordance with Article 20 in order to supplement this Regulation with technical requirements for the electronic means to be used by competent authorities for the transmission of removal orders.

2. The Commission shall be empowered to adopt such delegated acts to amend Annexes I, II and III in order to effectively address a possible need for improvements regarding the content of removal order forms and of forms to be used to provide information on the impossibility to execute the removal order.

Article 20
Exercise of delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 19 shall be conferred on the Commission for an indeterminate period of time from [*date of application of this Regulation*].

3. The delegation of power referred to in Article 19 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day after the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 19 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

www.parlament.gv.at

Article 21
Monitoring

1. Member States shall collect from their competent authorities and the hosting service providers under their jurisdiction and send to the Commission every year by [31 March] information about the actions they have taken in accordance with this Regulation. That information shall include:

   (a) information about the number of removal orders and referrals issued, the number of pieces of terrorist content which has been removed or access to it disabled, including the corresponding timeframes pursuant to Articles 4 and 5;

   (b) information about the specific proactive measures taken pursuant to Article 6, including the amount of terrorist content which has been removed or access to it disabled and the corresponding timeframes;

   (c) information about the number of complaint procedures initiated and actions taken by the hosting service providers pursuant to Article 10;

   (d) information about the number of redress procedures initiated and decisions taken by the competent authority in accordance with national law.

2. By [*one year from the date of application of this Regulation*] at the latest, the Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Regulation. The monitoring programme shall set out the indicators and the means by which and the intervals at which the data and other necessary evidence is to be collected. It shall specify the actions to be taken by the Commission and by the Member States in collecting and analysing the data and other evidence to monitor the progress and evaluate this Regulation pursuant to Article 23.

Article 22
Implementation report

By … [*two years after the entry into force of this Regulation*], the Commission shall report on the application of this Regulation to the European Parliament and the Council. Information on monitoring pursuant to Article 21 and information resulting from the transparency obligations pursuant to Article 8 shall be taken into account in the Commission report. Member States shall provide the Commission with the information necessary for the preparation of the report.

Article 23
Evaluation

No sooner than [*three years from the date of application of this Regulation*], the Commission shall carry out an evaluation of this Regulation and submit a report to the European Parliament and to the Council on the application of this Regulation including the functioning of the effectiveness of the safeguard mechanisms. Where appropriate, the report shall be accompanied by legislative proposals. Member States shall provide the Commission with the information necessary for the preparation of the report.

www.parlament.gv.at

Article 24
Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from [6 months after its entry into force].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

www.parlament.gv.at