Council of the European Union

Brussels, 3 December 2018
(OR. en)

14978/18

Interinstitutional File:
2018/0331(COD)

CT 194
ENFOPOL 595
JAI 1232
COTER 170
CYBER 303
TELECOM 440
FREMP 216
AUDIO 112
DROIPEN 189
CODEC 2160

NOTE

From:	Presidency
To:	Council
No. prev. doc.:	14570/18
Subject:	Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online - general approach

I. INTRODUCTION

1. On 12 September 2018, the Commission submitted to the Council a proposal for a Regulation on preventing the dissemination of terrorist content online[1], following a call for legislation from the European Council of June 2018 to improve the detection and removal of content inciting hatred and to commit terrorist acts. The proposal was part of the security package proposals accompanying the State of the Union speech by the President of the Commission.

[1] 12129/18 + ADD 1-3

2. The legal basis for the proposal is Article 114 of the Treaty of the Functioning of the European Union (internal market). The proposed Regulation creates the concept of removal orders obliging hosting service providers operating in the territory of the Union to take down terrorist content or disable access thereto within one hour. In case of non-compliance penalties can be imposed. The current text of the draft proposal contains strong safeguards to protect fundamental rights and principles, in particular the freedom of expression and the right to legal redress.

3. The current voluntary cooperation scheme, created through the EU Internet Forum, established in December 2015, will continue.

II. WORK WITHIN THE COUNCIL

4. The Terrorism Working Party (TWP) examined the draft Regulation at its meetings on 25 September, 5 and 25 October, and 6 and 15 November 2018. Following this thorough examination of the draft Directive at expert level, the JHA-Counsellors discussed some of the remaining issues on 22 November 2018. Furthermore, the draft Regulation was debated in CATS on 18 September 2018.

5. The Permanent Representatives Committee (COREPER) had a first debate during lunch on 26 September, exchanged views on counterterrorism issues, incl. this proposal with the EU Counter-Terrorism Coordinator at the COREPER breakfast of 21 November and examined the latest Presidency compromise proposal on 28 November 2018 with the Chair concluding that it had the required majority support.

III. MAIN ISSUES ADDRESSED

6. The Presidency compromise text addresses most of the issues raised by Member States by introducing a number of changes, addressed in "Article-order" below:

– In relation to fundamental rights and the need to protect journalistic content, the language on fundamental rights in general, and freedom of the press in particular, has been strengthened by introducing a new paragraph 3 to Article 1 and a substantial modification at the end of recital (9) to take into account the journalistic standards established by press or media regulation.

– In terms of scope, the definition of "*terrorist content*" in Article 2(5) has been more closely aligned with the Directive on combating terrorism. The definition of "*hosting service provider*" has been further clarified in recital (10) by setting out in detail the different constitutive elements of the definition, explaining which service providers would be outside of the scope and giving examples of hosting service providers covered.

– As regards the main instruments to prevent the dissemination of terrorist content online (Articles 4 and 5), the text clarifies in Article 4, paragraphs 3a) and 4 as well as in the corresponding recital (13a) which information shall be provided to the hosting service provider in the removal order. A new Article 4a) has been added setting out the consultation procedure for removal orders. An additional reference to the right for an effective remedy for removal orders has been introduced in recital (25) in addition to the general reference in recital (8).

– Regarding proactive measures, amendments to Article 6, paragraph 2a) and 4 now specify that it is up to the Member State to choose the nature and scope of these measures, when deciding on the proactive measures to be imposed.

– In response to the possible burden on small and medium sized companies, it has been specified in Article 8(2) and corresponding recital (24) that the requirement to publish transparency reports is limited to hosting service providers actually exposed to terrorist content.

– When, for reasons of public security, the obligation to disclose information of the removal of terrorist content to the content provider should not apply immediately, in Article 11(3), the period during which the information can be withheld, has been prolonged from 4 + 4 weeks to 6 + 6 weeks.

– Regarding cooperation, Article 13(3) and recitals (27) and (30) have been amended to ensure that Member States coordinate before issuing removal orders and referrals (clarifying how duplication and interference with investigations should be avoided) as well as to encourage the use of Europol tools. Article 13(4) has been amended to ensure that any notification of a serious threat would reach the right authority as soon as possible.

– Additionally, changes have been introduced to reduce the burden on hosting service providers, clarifying in recital (33) that the contact point pursuant to Article 14 for the processing of removal orders can be outsourced and limiting the 24/7 availability of a contact point to hosting service providers exposed to terrorist content.

– Article 15(3) on coercive measures and its corresponding recital (34a) have been deleted.

– In Article 24, the implementation period has been prolonged from six to twelve months.

With regard to the question of jurisdiction and the possible role of the Member State where the hosting service provider is established, including in relation to judicial redress, a number of changes were made. The current text clarifies in Article 15(1) and recital (34) that for reasons of effective implementation, urgency and public policy, any Member State has jurisdiction to issue removal orders and referrals to any hosting service provider, irrespective of the Member State where it is established or where it has designated a legal representative. Recital (27) clarifies that duplicate removal orders should not be issued. In addition, Article 4(a) has been added providing for the consultation of the competent authority of the Member State where the hosting service provider is established or has its legal representative. Finally, recital (38) clarifies that the Member State needs to ensure the full respect of fundamental rights before issuing penalties.

IV. OTHER ISSUES

7. The Czech Republic, Denmark and Finland maintain a parliamentary scrutiny reservation on the proposal.

8. The European Economic and Social Committee was consulted by the Council by letter of 24 October 2018 and will deliver its opinion during its December plenary session.

9. The European Parliament has appointed Ms Helga Stevens (ECR, BE), Committee on Civil Liberties, Justice and Home Affairs (LIBE), as rapporteur.

V. CONCLUSION

10. The Council is invited to adopt a general approach to the text, as set out in the Annex to this note.

11. Changes compared to the Commission proposal (12129/18) are marked: new text in ***bold italics;*** text deleted from the initial Commission proposal is indicated in ~~strikethrough~~.

ANNEX

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[2],

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] OJ C , , p. .

(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.

(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[3] 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.

[3] 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).

(5) The application of this Regulation should not affect the application of Article 14 of Directive 2000/31/EC[4]. 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. ***This Regulation does not apply to activities related to national security as this remains the sole responsibility of each Member State.***

(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.

---

[4] 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).

(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, ***as well as the freedom of the press and pluralism of the media,*** which constitute~~s 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 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 ***and for hosting service providers to contest a decision imposing proactive measures or penalities before the court of the Member State where they are established or have a legal representative***.

(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[5]. 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. ~~In addition, t~~***The definition includes content that provides guidance for the making and use of explosives, firearms or other weapons or noxious or hazardous substancesas well as CBRN substances, or on other methods and techniques, including the selection of targets, for the purpose of committing terrorist offences.*** Such ~~information~~ ***material*** 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,~~ ***counter-narrative*** or research purposes should be adequately protected***, striking a fair balance between fundamental rights including in particular the freedom of expression and information and public security needs***. ***Where the disseminated material is published under the editorial responsibility of the content provider, any decision as to the removal of such content should take into account the journalistic standards established by press or media regulation consistent with the law of the Union and the right to freedom of expression and the right to freedom and pluralism of the media as enshrined in Article 11 of the Charter of Fundamental Rights.*** Furthermore, the expression of radical, polemic or controversial views in the public debate on sensitive political questions should not be considered terrorist content.

---

5 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

(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 ***and material*** provided by a recipient of the service at his or her request and in making the information ***and material*** stored available to third parties, irrespective of whether this activity is of a mere technical, automatic and passive nature. ~~This Regulation applies to the activity of providing hosting services, rather than to the specific provider or its dominant activity, which might combine hosting services with other services that are not in the scope of this Regulation.~~ ***Storing content consists of holding data in the memory of a physical or virtual server; this excludes mere conduits and other electronic communication services within the meaning of [European Electronic Communication Code] or providers of caching services from scope, or other services provided in other layers of the Internet infrastructure, such as registries and registrars, DNS (domain name system) or adjacent services, such as payment services or DDoS (distributed denial of service) protection services. Further, the information has to be stored at the request of the content provider; only those services for which the content provider is the direct recipient are in scope. Finally, the information stored is made available to third parties, understood as any third user who is not the content provider. Interpersonal communication services that enable direct interpersonal and interactive exchange of information between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s), are not in scope.*** By way of example such ***hosting service*** providers ~~*of information society services*~~ include social media platforms, video streaming services, video, image and audio sharing services, file sharing and other cloud ***and storage*** services ~~*to the extent they make the information available to third parties and websites where users can make comments or post reviews*~~. ***This Regulation applies to the activity of providing hosting services, rather than to the specific provider or its dominant activity, which might combine hosting services with other services that are not in the scope of this Regulation***.

(10a) 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 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[6]. 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[7] cannot, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union.

---

6 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).

7 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).

(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 ***content***. 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 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. ***Without prejudice to the requirement to preserve data under Article 7 of this Regulation, or under the [draft e-evidence legislation], i***t 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. ***This should have the effect of preventing access or at least of making it difficult to achieve and of seriously discouraging internet users who are using their services from accessing the content to which access was disabled***.

(13a) The removal order should include a classification of the relevant content as terrorist content and contain sufficient information so as to locate the content, by providing a URL and any other additional information, such as a screenshot of the content in question. If requested, the competent authority should provide a supplementary statement of reasons, as to why the content is considered terrorist content. The reasons provided need not contain sensitive information which could jeopardise investigations. The statement of reasons should however allow the hosting service provider and, ultimately, the content provider to effectively exercise their right to judicial redress.

(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[8].

[8] 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).

(15) ~~Referrals by the competent authorities or Europol constitute a~~***n*** ~~effective and swift means of making hosting service providers aware of specific content on their services.~~ Th~~e~~***is referral*** mechanism of alerting hosting service providers to information ***and material*** that may be considered terrorist content, for the provider's voluntary consideration of the compatibility ***with*** its own terms and conditions***, constitutes a~~~~n~~*** ***particularly effective, and swift and proportionate means of making hosting service providers aware of specific content on their services*** ~~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[9] 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 ***risk or*** level of exposure to terrorist content.

---

[9] 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).

(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 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, ***'transactional data' and*** ~~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***, exposed to terrorists content,*** should publish annual transparency reports containing meaningful information about action taken in relation to the detection, identification and removal of terrorist content***, where it does not defeat the purpose of measures put in place***.

(25) Complaint procedures constitute a necessary safeguard against erroneous removal of content***, as a consequence of measures taken pursuant to the hosting service providers' terms and conditions*** 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. ***Furthermore, content providers, whose content has been removed following a removal order, should have a right to an effective remedy in accordance with Article 19 TEU and Article 47 of the Charter of Fundamental Rights of the European Union***.

(26) ***More generally, e*** ~~E~~ffective 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~~ ***before*** issuing removal orders or ***when*** sending referrals to hosting service providers. When deciding upon issuing thea removal order, the competent authority should give due consideration to any notification of an interference with an investigative interests ("de-confliction"). Where a competent authority is informed by a competent authority in another Member State of an existing removal order, a duplicate order should not be issued. ***When deciding upon issuing a removal order, the competent authority should give due consideration to any notification of an interference with an investigative interests ("de-confliction"). Where a competent authority is informed by a competent authority in another Member State of an existing removal order, a duplicate order should not be issued.*** 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. ***The Commission should facilitate such coordination and cooperation.***

(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~~ ***are encouraged to*** make use of ***the dedicated*** 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 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[10].

(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***, inhouse or outsourced,*** allowing for the electronic submission of removal orders and referrals and of technical ~~and~~ ***or*** 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 exposed to terrorist content, evidenced by the receipt of a removal order,*** 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. ***However, for reasons of effective implementation, urgency and public policy***, ***any Member State should have jurisdiction for removal orders and referrals.***

---

10 COM(2018)225 final.

(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. ***Hosting service providers may make use of an existing legal representative, provided that this legal representative is able to fulfil the functions as set out in 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 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***, which can be of an administrative or criminal nature,*** 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 assessing the nature of the breach and deciding upon applying penalties, full respect should be given to fundamental rights, such as the freedom of expression***. 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[11]. 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.

(41) Member States should collect information on the implementation of the legislation. ***Member States may make use of the hosting service providers' transparency reports and complement, where necessary, with more detailed information***. 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.

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

(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.

3. ***This Regulation shall not have the effect of modifying the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on the European Union.***

Article 2

Definitions

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

(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 establishment of the hosting service provider in the Union;

In the absence of such an establishment, the assessment of a substantial connection shall be based on specific factual criteria, such as

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

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

(4) 'terrorist offences' means ***one of the intentional acts listed*** ~~offences as defined~~ in Article 3(1) of Directive (EU) 2017/541;

(5) 'terrorist content' means ~~one or more of the following information~~ ***material which may contribute to the commission of the intentional acts, as listed in Article 3(1)(a) to (i) of the Directive 2017/541, by***:

(aa) threatening to commit a terrorist offence;

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

(b) ***soliciting persons or a group of persons to commit or*** ~~encouraging the~~ contribut***eion*** ~~eion~~ to terrorist offences;

(c) promoting the activities of a terrorist group, in particular by ***soliciting persons or a group of persons to*** ~~encouraging the~~ participat***eion*** ~~ion~~ in or support ***the criminal activities of*** ~~to~~ a terrorist group within the meaning of Article 2(3) of Directive (EU) 2017/541;

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 ***in the Union***.

SECTION II

MEASURES TO PREVENT THE DISSEMINATION OF TERRORIST CONTENT ONLINE

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 ***that they will not store terrorist content***, 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~~ ***removal order*** 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;~~a statement of reasons explaining why the content is considered terrorist content,~~ ***an assessment of the content,*** at least, by reference to the ***relevant*** categories of terrorist content listed in Article 2(5);

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

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

(d) date and time stamp of issuing;

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

(f) 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~~ ***supplementary*** statement of reasons, ***explaining why the content is considered terrorist content*** 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 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. ***Without undue delay, h***~~H~~osting 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 4(a)

Consultation procedure for removal orders

1. The issuing authority shall submit a copy of the removal order to the competent authority referred to in Article 17(1)(a) of the Member State in which the main establishment of the hosting service provider is located at the same time it is transmitted to the hosting service provider in accordance with Article 4(5).

2. In cases where the competent authority of the Member State in which the main establishment of the hosting service provider is located has reasonable grounds to believe that the removal order may impact fundamental interests of that Member State, it shall inform the issuing competent authority.

3. The issuing authority shall take these circumstances into account and shall, where necessary, withdraw or adapt the removal order.

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 sufficient~~ly detailed~~ information~~, including~~ ***on*** the reasons why the content is considered terrorist content, ***and provide*** a URL and, where necessary, additional information enabling the identification of the terrorist content referred.

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***, without undue delay,*** ~~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,~~ ***depending on the risk and level of exposure to terrorist content,*** 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~~ ***effectively address*** the re***appearance*** ~~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.

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. ***It shall be to the discretion of the competent authority referred to in Article 17(1)(c) to decide on the nature and the scope of the proactive measures, in accordance with the aim of this Regulation***. 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 meaningful explanation of the functioning of proactive measures including the use of automated tools.

2. Hosting service providers, ~~where applicable~~ ***exposed to terrorist content,*** 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 ***effectively address*** ~~prevent~~ the re~~-upload~~***appearance*** 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.

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~~ ***six***~~]~~ weeks from that decision. ***This period can be prolonged once for another six weeks, where justified.*** 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*~~ ***competent*** *Union bodies*

1. Competent authorities in Member States shall inform, coordinate and cooperate with each other and, where appropriate, with ~~relevant~~ ***competent*** 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. ***For the effective implementation of this Regulation as well as to avoid duplication,*** Member States and hosting service providers may choose to make use of dedicated tools, including~~, where appropriate,~~ those established by ~~relevant~~ ***competent*** Union bodies such as Europol, to facilitate in particular:

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

   (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***(s)*** ~~or the point of contact in the Member State pursuant to Article 14(2), where they have their main establishment or a legal representative~~. ***Where it is impossible to identify the Member State(s) concerned, the h***~~H~~Hosting service providers ~~may, in case of doubt,~~ ***shall notify the point of contact in the Member State pursuant to Article 14(3), where they have their main establishment or a legal representative, and also*** 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 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. ***Any Member State shall have jurisdiction for the purposes of Articles 4 and 5, irrespective of where the hosting service provider has its main establishment or has designated a legal representative.***

2. Where a hosting service provider fails to designate a legal representative, all Member States shall have jurisdiction. ***Where a Member State decides to exercise jurisdiction, it shall inform all other Member States***.

~~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.~~

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 [***twelve*** ~~*six*~~ *months after the entry into force of this Regulation*] at the latest Member States shall notify the Commission of the competent ***authority or*** 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*.

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 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 ***or natural*** person held responsible;

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

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

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.

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.

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 [***12*** ~~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*