Council of the European Union

Brussels, 27 January 2021
(OR. en)

5634/21

Interinstitutional File:
2018/0331(COD)

CT 7
ENFOPOL 30
COTER 13
JAI 63
CYBER 17
TELECOM 27
FREMP 12
AUDIO 9
DROIPEN 12
CODEC 107

'I' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee (Part 2)
No. prev. doc.:	12906/20
Subject:	Proposal for a Regulation on addressing the dissemination of terrorist content online – *Confirmation of the final compromise text with a view to agreement*

1. On 16 December 2020, COREPER analysed the compromise agreement reached with the European Parliament on the proposal for a Regulation on addressing the dissemination of terrorist content online, as set out in 12906/20.

2. On 11 January 2021, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) sent a letter to the Presidency. On 13 January, the Presidency of the Council received the attached offer letter (see Annex I) from the chairman of the LIBE informing that, if this text was to be transmitted formally to the European Parliament as the Council's First Reading Position for this legislative proposal, he would recommend to the Members of LIBE and subsequently to the Plenary that the Council's First Reading Position be accepted without amendments in Parliament's second reading, subject to verification by the lawyer linguists of both institutions.

3. The Permanent Representatives Committee is invited to confirm the final compromise on the on the proposal for a Regulation on addressing the dissemination of terrorist content online, as voted by the LIBE Committee (see Annex II).

European Parliament

Committee on Civil Liberties, Justice and Home Affairs
The Chairman

IPOL-COM-LIBE D (2021) 605

Mr. Nuno Brito
Ambassador,
Permanent Representative of Portugal
Council of the European Union
Avenue de Cortenbergh 12
1040 Brussels

D 300116 13.01.2021

Subject: Council's First Reading Position on the proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (2018/0331(COD))

Dear Ambassador Brito,

Following the vote on a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online that took place in the meeting of the Committee on Civil Liberties, Justice and Home Affairs of 11 January 2021, I would like to inform you that the LIBE Committee considered positively the acceptance of the text set out in the Annex which reflects the outcome of the negotiations between the three Institutions.

Thus, I would like to inform you that, if this text was to be transmitted formally to the European Parliament as the Council's First Reading Position for this legislative proposal, I will recommend to the Members of the Committee on Civil Liberties, Justice and Home Affairs and subsequently to the Plenary that the Council's First Reading Position be accepted without amendments in Parliament's second reading, subject to verification by the lawyer linguists of both institutions.

I would like to thank you and the previous Council Presidencies for the close cooperation on this file.

Yours sincerely,

Juan Fernando López Aguilar

Annex: text agreed

B-1047 Brussels - Tel. +32 2 28 40660
F-67070 Strasbourg - Tel. +33 3 88 1 74420

ANNEX II

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on ~~preventing~~ addressing the dissemination of terrorist content online

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[1],

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~~ **addressing** the misuse of hosting services for terrorist purposes **and contributing to public security in European societies**. 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~~ **including the freedom to receive and impart** information **and ideas in an open and democratic society and to the freedom and pluralism of the media**.

[1] OJ C , , p. .

(1a) Regulatory measures to address the dissemination of terrorist content online should be complemented by Member States' strategies to address terrorism, including measures such as strengthening of media literacy and critical thinking, alternative and counter narratives and other initiatives to reduce the impact of and vulnerability to terrorist content online as well as investment in social work, de-radicalisation initiatives and engagement with affected communities to achieve a sustainable prevention of radicalisation in society.

(1b) Terrorist content is part of a broader problem of illegal content online, which requires a combination of legislative, non-legislative and voluntary measures based on collaboration between authorities and hosting service providers, in the full respect for fundamental rights.

(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) **While not the only factor, t**~~T~~he presence of terrorist content online **has proven to be a catalyst for the radicalisation of individuals which can lead to terrorist acts, and therefore** 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~~ **address** terrorist content disseminated through their services**, whilst taking into account the fundamental importance of the freedom of expression, including the freedom to receive and impart information and ideas in an open and democratic society**.

(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[2] and responds to calls made by the European Parliament to strengthen measures to tackle illegal and harmful content **in line with the horizontal framework established by Directive 2000/31/EC** 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[3]. In particular, any measures taken by the hosting service provider in compliance with this Regulation, including any **specific** ~~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~~ **address** 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~~ **and should fully** 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.

---

[2] 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).

[3] 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 **seeks to** contribute~~s~~ 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 **are** ~~is one of~~ the values on which the Union is founded. Measures ~~constituting interference in~~ **affecting** the freedom of expression and information should be strictly targeted, in the sense that they must serve to ~~prevent~~ **address** 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. **Effective online counterterrorism measures and the protection of freedom of expression are not conflicting, but complementary and mutually reinforcing goals.**

(8) *Now recital (24b)*

(9) In order to provide clarity about the actions that both hosting service providers and competent authorities should take to ~~prevent~~ **address** the dissemination of terrorist content online, this Regulation should establish a definition of terrorist content for preventative purposes ~~drawing on~~ **aligned to** the definition of terrorist offences under Directive (EU) 2017/541 of the European Parliament and of the Council. Given the need to address the most harmful terrorist propaganda online, the definition should capture material ~~and information~~ that incites~~, encourages~~ or ~~advocates~~ **solicits** the commission **of** or **the** contribution to terrorist offences, ~~provides instructions for the commission of such offences~~ or **solicits** ~~promotes~~ the participation in activities of a terrorist group **or glorifies terrorist activities, including by disseminating material depicting a terrorist attack**. ~~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 chemical, biological, radiological and nuclear (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**, as well as of live transmissions of terrorist offences thereby causing a danger that further such offences may be committed**. 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.

(9a) Content disseminated for educational, journalistic, **artistic** or research purposes or for **awareness-raising purposes against terrorist activity** should ~~be adequately protected~~ **not be considered terrorist content**. **When determining whether information provided by a content provider constitutes 'terrorist content' within this Regulation account should be taken of in particular the freedom of expression and information, the freedom of the arts and sciences, and the freedom and pluralism of the media. Especially in cases where the content provider holds an editorial responsibility, any decision as to the removal of the disseminated material should take into account the journalistic standards established by press or media regulation consistent with the law of the Union and 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.

(9b) In case of conflict between this Regulation and Directive 2010/13/EU in relation to provisions governing audiovisual media services as defined in its Article 1(1)(a), the AVMS-Directive (Directive 2010/13/EU) should prevail. This leaves the obligations, in particular of providers of video sharing platform services under this Regulation unaffected.

(10) In order to **effectively address** ~~cover those online hosting services where~~ terrorist content **online** ~~is disseminated~~, **while ensuring respect for the private life of individuals,** this Regulation should apply to **providers of** information society services which store **and disseminate to the public** information **and material** 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 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.~~ **The concept of "storage" should be understood as holding data in the memory of a physical or virtual server. Providers of "mere conduit" or "caching" services as well as of other services provided in other layers of the internet infrastructure, which do not involve such storage, such as registries and registrars as well as providers of domain name systems (DNS), payment or distributed denial of service (DdoS) protection services therefore fall outside the scope of this Regulation.**

(10a) **The concept of "*dissemination to the public*" should entail the making available of information to a potentially unlimited number of persons that is, making the information easily accessible to users in general without further action by the content provider being required, irrespective of whether those persons actually access the information in question. Accordingly, where access to information requires registration or admittance to a group of users, it should be considered to be disseminated to the public only where users seeking to access the information are automatically registered or admitted without a human decision or selection of whom to grant access. Interpersonal communication services, as defined in the Directive 2018/1972 establishing the European Electronic Communications Code[4] such as emails or private messaging services, fall outside the scope of this Regulation. Information should be considered stored and disseminated to the public within the meaning of this Regulation only where such activities are performed upon direct request by the content provider. Consequently, providers of services such as cloud infrastructure, which are provided at the request of other parties than the content providers and only indirectly benefit the latter, should not be covered by this Regulation. By way of example, included in the scope of this Regulation are providers of social media, video, image and audio-sharing, as well as file-sharing and other cloud services, in as far as those services are used to make the stored information available to the public at the direct request of the content provider. Where a service provider offers several services, this Regulation should be applied only in respect of the services that fall within its scope.**

4 OJ L 321, 17.12.2018, p. 36.

(10b) Terrorist content is often disseminated to the public through services provided by service providers established in third countries. In order to protect users in the Union and to ensure that all service providers operating in the Digital Single Market are subject to the same requirements, this Regulation should apply to all providers of relevant services offered in the Union, irrespective of their country of main establishment. The determination as to whether a service provider offers services in the Union requires an assessment whether it enables legal or natural persons in one or more Member States to use its services and has a substantial connection to that Member State or Member States, However, the mere accessibility of a service provider's website or of an email address or 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~~, or the possibility of ordering goods or services.~~ 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[5]. 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[6] cannot, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union.

(12) *Moved down before recital (16)*

---

5 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).

6 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).

(13) The procedure and obligations resulting from ~~legal~~ **removal** orders ~~requesting~~ **requiring** 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 **in all Member States** within one hour from receiving the removal order. **In duly justified emergency cases, the competent authority may issue the first removal order to a hosting service provider without having provided information on procedures and applicable deadlines 12 hours in advance. Such emergency cases occur where a removal of or disabling of access to the content later than one hour after notification would result in serious harm, such as in a situations of an imminent threat to life or the physical integrity of a person or events depicting ongoing harm to life or physical integrity. It is for the competent authority to establish such an emergency case and provide the necessary justification. In case the hosting service provider cannot comply with the removal order within one hour, because of force majeure or of de facto impossibility, it should inform the authorities as soon as possible and comply with the removal order as soon as the reasons for the impossibility are no longer present. Such reasons could also be of technical or operational nature.**

(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 an exact URL and, where necessary, any other additional information, such as a screenshot of the content in question. 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~~ **contact** point ~~of contact~~ **of the hosting service provider** 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[7]. **Where the hosting service provider's main establishment is in another Member State, a copy of that order should at the same time be transmitted to the competent authority of that Member State.**

(14a) The competent authority of the Member State where the hosting service provider has its main establishment or legal representative should have the possibility to scrutinise the removal order issued by competent authorities from another Member State to determine whether or not it seriously or manifestly violates the Regulation or involves serious or manifest breaches of fundamental rights as enshrined in the Charter. Both the content provider and the hosting service provider should have the right to request a review by the competent authority in the Member State where the hosting service provider has its main establishment or legal representative, in which case the relevant authority is under an obligation to adopt a decision on whether or not the removal order contains such violations and breaches. Where the relevant authority finds such violations and breaches, the removal order should cease to have legal effects. The scrutiny should be carried out swiftly so as to ensure that erroneously removed content is reinstated quickly.

[7] 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. Thiese~~ ***~~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 an 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~~[8] ~~remains unaffected.~~

(former recital (12)

Hosting service providers **that are exposed to terrorist content should, where they have terms and conditions, include therein provisions to address the misuse of their services for the dissemination to the public of terrorist content.** They 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~~**those** in a diligent, **transparent** 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~~.

[8] 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).

(16) Given the scale and speed necessary for effectively identifying and removing terrorist content, proportionate **and effective specific** ~~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 **exposed to terrorist content** should ~~assess whether it is appropriate to~~ take ~~proactive~~ **specific** measures **taking into account** 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~~**H**~~h~~osting service providers should determine what appropriate, effective and proportionate ~~proactive~~ **specific** measure should be put in place **to identify and remove terrorist content**. ~~This requirement should not imply a general monitoring obligation.~~ **Specific measures may include appropriate technical or operational measures or capacities such as staffing or technical means to identify and expeditiously remove or disable access to terrorist content, mechanisms for users to report or flag alleged terrorist content or any other measures the hosting service provider considers appropriate and effective to address the availability of terrorist content on its services.** ~~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.~~

(17) When putting in place ~~proactive~~ **specific** measures, hosting service providers should ensure that users' right to freedom of expression and information **as well as the freedom and pluralism of the media as protected under the EU-Charter** ~~– 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, **where appropriate,** 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 **hosting** service provider should report on the ~~proactive~~ **specific** 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 **size and** economic capacity and the impact of its service in disseminating terrorist content (for example, taking into account the number of users in the Union*)* **as well as the safeguards put in place to address the misuse of their services for the dissemination of terrorist content online**.

(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~~ **require** the adoption of **additional** appropriate, effective and proportionate ~~proactive~~ **specific** measures where it considers that the measures taken are insufficient to meet the risks. ~~A decision to impose~~**The requirement to implement** such **specific** ~~proactive~~ measures should not lead to ~~the imposition of~~ a**n** ~~general~~ obligation to monitor, as provided in Article 15(1) of Directive 2000/31/EC **nor an obligation to use automated tools. Hosting service providers may however decide to use automated tools if they consider this appropriate and necessary to effectively address the misuse of their services for the dissemination of terrorist content.** ~~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, 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 **or remedy** 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 terrorist content and the related data should be stored only for a specific period allowing the law enforcement authorities to check the content and decide whether it would be needed for those specific purposes. For the purposes of prevention, detection, investigation and prosecution of terrorist offences**, 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. Where companies remove material or disable access to it, in particular through their own ~~proactive~~ **specific** measures, ~~and do not~~ **they should** inform the ~~relevant~~ **competent** authorit~~y~~**ies promptly about content that contains information leading to or resulting in an imment threat to life or a suspected terrorist offence**.

(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~~ **or** to enable law enforcement **authorities'** 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 **or remedy** 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~~ **material** in relation to investigations **and prosecutions**, 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 **that have taken action against or were required to take action pursuant to this Regulation on the dissemination of terrorist content in a given calendar year,** should publish annual transparency reports containing meaningful information about action taken in relation to the ~~detection,~~ identification and removal of terrorist content.

(24a) The competent authorities of the Member States should publish transparency reports containing information on the number of removal orders, the number of refusals and the number of decisions concerning specific measures, the number of decisions imposing penalties and the number of cases subject to administrative or judicial review.

(24b) *Moved from recital (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 **or any decisions resulting from the scrutiny of removal orders under this Regulation** before the court of the Member State whose authorities issued the removal order **respectively took the decision, as well as for hosting service providers to effectively contest a decision relating to specific measures or penalties before the court of the Member State whose authority took that decision**.

(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.

(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 **and to minimise the expenses of the affected service providers**, the competent authorities should inform, coordinate and cooperate with each other and where appropriate with Europol ~~when~~ **before** issuing removal orders ~~or sending referrals~~ to hosting service providers. **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~~ **specific** measures **taken by hosting service providers**, competent authorities in Member States should liaise with each other with regard to the discussions they have with hosting service providers as to **removal orders and** 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 authorit~~y~~**ies in other Member States**. For that purpose, Member States should ensure appropriate **and secure** 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.

(30a) **Referrals by Member States and Europol have proven to be an effective and swift means of increasing the hosting service providers' awareness of specific content on their services and enabling them to take swift action. This mechanism of alerting hosting service providers to information that may be considered terrorist content, for the provider's voluntary consideration of the compatibility with its own terms and conditions, should remain available in addition to removal orders. 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, Europol's mandate as laid down in Regulation (EU) 2016/7941 remains unaffected. Therefore, nothing in this Regulation should be understood as precluding the Member States and Europol from using referrals as an instrument to address terrorist content.**

(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 **content that contains information leading to or resulting in an imment threat to life or a suspected terrorist offence** ~~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~~.

(33) ~~Both h~~**H**osting service providers ~~and Member States~~[9] should establish points of contact to facilitate the ~~swift~~ **expeditious** 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~~ **expeditious** 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, **it is necessary that** the point of contact of hosting service providers **exposed to terrorist content, evidenced by the receipt of a removal order,** 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.

[9] Presidency suggests to delete Member States in this recital, since Article 14 covers only contact points of the Hosting Service Providers after revisions.

(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. **That should be without prejudice to the rules on competence established for the purpose of removal orders and decisions resulting from the scrutiny of removal orders under this Regulation**. ~~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. **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 necess**itate**~~arily require~~ the establishment of **a** new authorit**y**~~*ies*~~ but can be **an** existing bod**y**~~ies~~ tasked with the functions set out in this Regulation. This Regulation requires designating authorities competent for issuing removal orders, **scrutinising removal orders** ~~referrals~~ and for overseeing ~~proactive~~ **specific** measures and for imposing penalties. It is for Member States to decide how many authorities they wish to designate for these tasks **allowing them to designate administrative, law enforcement or judicial authorities with that task**. **Member States should ensure that the competent authorities fulfill their tasks in an objective and non-discriminatory manner and do not seek or take instructions from any other body in relation to the exercise of the tasks assigned to them by this regulation. This does not prevent supervision in accordance with national constitutional law. Member States should communicate the competent authority designated under this Regulation to the Commission, which should publish on-line a compilation of the competent authority of each Member State. The online registry should be easily accessible to facilitate the swift verification of the authenticity of removal orders by the hosting service providers.**

(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~~ **should** 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. **Penalties can take different forms including formal warnings in cases of minor breaches or financial penalties in relation to more severe or systematic breaches**. In order to ensure legal certainty, the~~r~~**is** ~~r~~**R**egulation 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. **Moreover, the competent authority should take into account whether the hosting service provider is a start-up or a small and medium sized business. Additional circumstances such as whether the conduct of the hosting service provider was objectively imprudent or reprehensible or whether the infringement has been committed negligently or intentionally should also be taken into account.** Member States ~~shall~~ **should** 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[10]. 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, such as own transparency reports as a consequence of this Regulation**. 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.

[10] 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~~ **two** years[11] after its entry into force. The evaluation should be based on the ~~five~~ criteria of efficiency, **necessity, proportionality,** effectiveness, relevance, coherence and EU added value. It ~~will~~ **should** 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 **fundamental** rights**, including the freedom of expression and freedom to receive and impart information, the freedom and pluralism of the media, the freedom to conduct a business and the rights to privacy and the protection of personal data. The Commission should also assess the impact on potentially affected** ~~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~~ **addressing** 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:

---

11 As agreed, see Article 23.

SECTION I
GENERAL PROVISIONS

Article 1

Subject matter and scope

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

   (a) rules on **reasonable and proportionate** duties of care to be applied by hosting service providers in order to **address** ~~prevent~~ the dissemination **to the public** 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, **in accordance with Union law and subject to suitable safeguards to protect fundamental rights, in particular the freedom of expression and information in an open and democratic society,** 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, **which disseminate information to the public**.

2a Material disseminated for educational, journalistic, artistic or research purposes or for the purposes of preventing or countering terrorism, including the content which represents an expression of polemic or controversial views in the course of public debate shall not be considered terrorist content. An assessment shall determine the true purpose of dissemination and examine whether material is disseminated for the purposes referred to in this paragraph.

2b This Regulation shall not have the effect of modifying the obligation to respect the rights, freedoms and principles as referred to in Article 6 of the Treaty on the European Union, and shall apply without prejudice to fundamental principles relating to freedom of speech, freedom of the press and the freedom and pluralism of the media.

2c This Regulation shall be without prejudice to Directive 2000/31/EC and to Directive 2010/13/EU. For audiovisual media services as defined in Article 1(1)(a) of Directive 2010/13/EU the Directive 2010/13/EU shall prevail.

Article 2

Definitions

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

(1) 'information society services' means the services as referred to in point (b) of Article 1 of Directive (EU) 2000/31/EC;

(2) '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~~;

(3) 'content provider' means a user who has provided information that is, or that has been, stored **and made available to the public** at the request of the user by a hosting service provider;

(4) '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**;

Such a substantial connection shall be deemed to exist where the hosting service provider has an establishment 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) establishment of the hosting service provider in the Union;

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

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

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

(6) 'terrorist content' means one or more of the following information **material**:

(a) inciting or advocating, including **the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, where such material, directly or indirectly such as** by **the glorification** glorifying **of terrorist acts, advocates** the commission of terrorist offences, thereby causing a danger that **one or more** such acts **offences may** be committed;

(b) **soliciting a person or a group of persons to commit or** encouraging the contribut**c**ion to **the commission of one of the** terrorist offences**, referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541**;

(c) promoting**soliciting a person or a group of persons to participate in** the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Article **4** 2(3) of Directive (EU) 2017/541;

(d) **providing** instructi~~n~~g**on** on **the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific** methods or techniques for the purpose of committing **or contributing to the commission of one of the** terrorist offences **referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;**

(e) **constituting a threat to commit one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541.**

(7) 'dissemination **to the public** ~~of terrorist content~~' means **the** making **available of information, at the request of the content provider, to a potentially unlimited number of persons** ~~terrorist content available to third parties on the hosting service providers' services~~;

(8) '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;

~~(9) '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;~~

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

SECTION II

MEASURES TO ADDRESS THE DISSEMINATION OF TERRORIST CONTENT ONLINE

~~*Article 3*~~[12]

~~*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 **of any Member State** shall have the power to issue a ~~decision~~ removal order **to any hosting service provider offering services within the Union** requiring the hosting service provider to remove content or disable access to it **in all Member States**.

1a. If the issuing competent authority is in a different Member State than where the hosting service provider is established or has its legal representative, Article 4a shall apply additionally.

1b. **If the relevant competent authority has not previously issued a removal order to a hosting service provider it shall provide the hosting service provider with information on procedures and applicable deadlines at least 12 hours before issuing a removal order except in duly justified emergency cases.**

[12] Article 3 has been merged with Articles 6 and 9 into a new Article X.

2. Hosting service providers shall remove terrorist content or disable access to it **in all Member States as soon as possible and in any event** within one hour from receipt of the removal order **pursuant to paragraph 1**.

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

(a) identification of the competent authority **via an electronic signature** issuing the removal order and authentication of the removal order by the competent authority;

(b) a **sufficiently detailed** statement of reasons explaining why the content is considered terrorist content, ~~at least, by~~ **and a** reference to the **relevant** categories of terrorist content listed in Article 2(5)

(c) a**n exact** 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) **easily understandable** information about redress available to the hosting service provider and to the content provider, **including redress with the competent authority, as well as recourse to a court as well as deadlines for appeal**;

(g) where ~~relevant~~ **necessary and proportionate**, 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 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 **inform** ~~acknowledge receipt and~~, without undue delay, ~~inform~~ the competent authority about the removal of terrorist content or disabling access to it **in all Member States**, 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 **including for objectively justifiable technical and operational reasons**, 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 **specific** ~~proactive~~ measures, referred to in Article 17(1)(c) when the removal order becomes final. A removal order **shall** become~~s~~ final **upon the expiry of** ~~where it has not been appealed within~~ the deadline **for appeal under** ~~according to the applicable~~ national law or where it has been confirmed following an appeal.

Article 4a

Procedure for cross border removal orders

1. Where the hosting service provider does not have its main establishment or legal representative in the Member State of the issuing competent authority, the issuing competent authority shall, at the same time, submit a copy of the removal order to the competent authority of the Member State where the hosting service provider has its main establishment or legal representative.

2. Where a hosting service provider receives a removal order covered by this Article, it shall take the measures required by Article 4 and, in addition, take the necessary measures to be able to reinstate, or re-able access to, the content in question, in accordance with paragraph 4.

3. The competent authority of the Member State where the hosting service provider has its main establishment or its legal representative may, within 72 hour from receiving the copy of the removal order pursuant to paragraph 1 scrutinise the removal order to determine whether or not it seriously or manifestly violates this Regulation or involves any serious or manifest breaches of the fundamental rights and freedoms guaranteed by the Charter and, where it finds that there are such violations or breaches, it shall adopt a reasoned decision to that effect.

That competent authority shall, within 72 hours from receiving the request referred to in paragraph 5, carry out that scrutiny and adopt a reasoned decision setting out its findings as to whether or not there are such violations or breaches.

The competent authority shall, before adopting the decisions referred to in the first and second subparagraphs, inform the issuing competent authority on its intention to adopt the decision and the reasons for doing so.

4. Where the competent authority of the Member State where the hosting service provider has its main establishment or its legal representative adopts a reasoned decision pursuant to paragraph 3, it shall, without delay, communicate that decision to the issuing authority, the hosting service provider, the content provider, who requested the scrutiny pursuant to paragraph 5 and, in accordance with Article 13, to Europol. If the decision finds violations or breaches pursuant to paragraph 3, the removal order shall cease to have legal effects.

The hosting service provider concerned shall, immediately, reinstate, or re-enable access to, the content in question, without prejudice to the possibility to enforce its terms and conditions in accordance with Union and national law.

5. A hosting service provider and a content provider shall be entitled to submit, within 48 hours from receiving the removal order or information pursuant to Article 11 (2) respectively, a reasoned request to the competent authorities of the Member State where the hosting service provider has its main establishment or its legal representative to exercise the right of scrutiny referred to in paragraph 3.

~~*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 ***on*** the reasons why the content is considered terrorist content, 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 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* [13]~~

~~*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.~~

[13] Article 6 has been merged with Articles 3 and Article 9 into the new Article X.

~~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 address 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.~~

~~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 X (merging Articles 3, 6 and 9)

Specific measures

1. Hosting service providers exposed to terrorist content shall, where applicable, include in their terms and conditions, and apply, provisions to address the misuse of their service for the dissemination to the public of terrorist content online. They shall do so in a diligent, proportionate and non-discriminatory manner, and with due regard in all circumstances 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 and with a view to avoiding the removal of material which is not terrorist content.

2. Where a hosting service provider is exposed to terrorist content in accordance with paragraph 4, it shall take specific measures to protect their services against the dissemination to the public of terrorist content.

The decision as to the choice of specific measures shall remain with the hosting service provider. Those measures may include one or more of the following:

(a) appropriate technical and operational measures or capacities such as appropriate staffing or technical means to identify and expeditiously remove or disable access to terrorist content;

(b) easily accessible and user-friendly mechanisms for users to report or flag to the hosting service provider alleged terrorist content;

(c) any other mechanisms to increase the awareness of terrorist content on its services such as mechanisms for users moderation;

(d) any other measure that the hosting service provider considers appropriate to address the availability of terrorist content on its services.

3. Any specific measure or measures that a hosting service provider takes pursuant to paragraph 2 shall meet all of the following requirements:

(a) they shall be effective in mitigating the level of exposure to terrorist content;

(b) they shall be targeted and proportionate, taking into account, in particular, the seriousness of the level of exposure to terrorist content as well as the technical and operational capabilities, financial strength, the number of users of the hosting service provider and the amount of content they provide;

(c) they shall be applied taking full account of the rights and legitimate interest of the users, in particular users' fundamental rights to freedom of expression and of information, to respect for private life and to protection of personal data;

(d) they shall be applied in a diligent and non-discriminatory manner;

Where they involve the use of technical measures, appropriate and effective safeguards shall be provided to ensure accuracy and to avoid the removal of information that is not terrorist content, in particular through human oversight and verification.

4. For the purposes of paragraph 2, a hosting service provider shall be considered to be exposed to terrorist content, where the competent authority of the Member State of its main establishment has informed the hosting service provider, through a decision based on objective factors, such as the hosting service provider having received two or more final removal orders in the previous 12 months that it considers the hosting service provider to be exposed to terrorist content.

5. After having received the decision referred to in paragraph 4 and, where relevant, paragraph 6, a hosting service provider shall report to the competent authority on the specific measures it has taken and that it intends to take in order to comply with the requirement laid down in paragraphs 2 and 3. It shall do so within three months of receipt of the decision and on an annual basis thereafter. This obligation ceases once the competent authority has confirmed that the hosting service provider is no longer obliged pursuant to paragraph 2 after a request pursuant to paragraph 7.

6. Where, based on the reports referred to in paragraph 5 and, where relevant, any other objective factors, the competent authority considers that the measures that a hosting provider has taken do not meet the requirements of paragraphs 2 and 3, the competent authority shall address a decision to the hosting service provider requiring it to take the necessary measures so as to ensure that those requirements are met. The decision as to the choice of measures remains with the hosting service provider.

7. A hosting service provider may, at any time, request the competent authority to review and, where appropriate, adjust or revoke the decisions referred to in paragraphs 4 and 6. The competent authority shall, within three months of receipt of the request, take a reasoned decision based on objective factors on the request and inform the hosting service provider accordingly.

8. Any requirement to take measures pursuant to this Article shall be without prejudice to Article 15 of Directive 2000/31/EC and shall not entail a general obligation on hosting services providers to monitor the information, which they store, nor a general obligation to actively seek facts or circumstances indicating illegal activity. Any requirement to take measures pursuant to this Article shall not include an obligation to use automated tools 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 **specific** ~~proactive~~ measures pursuant to Article~~s~~ 4~~, 5 and 6~~ X 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~~ **remedy, complaint-handling in respect of the decision to remove or disable access to terrorist content and related data,**

   (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~~ **further specified** period ~~when~~ **only if** and for as long as necessary for ongoing proceedings of administrative or judicial ~~review~~ **remedies** 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 **for hosting service providers***

1. Hosting service providers shall set out **clearly** in their terms and conditions their policy to **address** ~~prevent~~ the dissemination of terrorist content, including, where appropriate, a meaningful explanation of the functioning of **specific** ~~proactive~~ measures including, **where applicable,** the use of automated tools.

2. **Any h**~~H~~osting service provider~~s~~, **that has taken action against the dissemination of terrorist content or has been required to take action pursuant to this Regulation in a given calendar year**, shall ~~publish annual~~ **make publicly available a** transparency report~~s~~ on action taken against the dissemination of terrorist content **for that period**. **They shall publish those reports within two months from the end of that year**.

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 **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, **in particular where automated tools have been used;**

   (c) number of pieces of terrorist content removed or to which access has been disabled, following removal orders~~, referrals,~~ or **specific** ~~proactive~~ measures, respectively, **and the number of orders where the content has not been removed in accordance with Article 4(7) and (8) together with reasons for non-removal;**

(d) ~~overview~~ **number** and outcome of complaint**s** ~~procedures~~ **processed by the hosting service provider, as well as number and outcome of actions for judicial or administrative remedy initiated by the hosting service provider, and number of cases in which the hosting service provider was required to reinstate the content as a result of a judicial or administrative remedy, or where the hosting service provider reinstated the content after examining a complaint by the content provider.**

Art 8(a)

Transparency obligations for competent authorities

1. Competent authorities shall publish annual transparency reports relating to their activities under this Regulation. Those reports shall include at least the following information in relation to the year covered:

(a) the total number of removal orders issued in accordance with Article 4 and scrutinised under Article 4a, and information on the effects given to those orders by the hosting service providers concerned, including the number of instances in which the removal orders led to the removal of or disabling of access to terrorist content and the number of instances in which they did not;

(b) the total number of decisions taken in accordance with Article X(4) and information on the effects given to those decisions by hosting service providers, including a description of the measures imposed;

(c) the total number of instances in which removal orders and decisions taken in accordance with Article X(4) were subject to administrative or judicial review and information on the outcome of the relevant proceedings.

(d) the total number of decisions imposing penalties, including a description of the type of penalty imposed.

2. The transparency reports referred to in paragraph 1 shall not contain information that may affect ongoing activities for the prevention, detection investigation or prosecution of terrorist offences or national security interests.

~~*Article 9*~~[14]

~~*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 9 a

Effective remedies

1. Hosting service providers that have received a removal order pursuant to Article 4(1), a decision pursuant to Article 4a(3) or a decision pursuant to Article X(4), (6) and (7) shall have a right to an effective remedy. This shall include a right to challenge the removal order issued pursuant to Article 4(1), or the decision pursuant to Article 4a(3), before the courts of the Member State that issued the removal order or took that decision.

2. Content providers whose content has been removed or access to which has been disabled following a removal order shall have the right to an effective remedy. This shall include the right to challenge the removal order issued pursuant to Article 4(1) or a decision pursuant to Article 4a(3) before the courts of the Member State which issued the removal order or took that decision.

3. Member States shall put in place effective procedures for exercising the rights referred to in paragraphs 1 and 2.

---

14 Article 9 has been merged with Articles 3 and 6 into the new Article X.

Article 10

Complaint mechanisms

1. Hosting service providers shall establish **an** effective and accessible mechanism~~s~~ 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~~ **specific** measures pursuant to Article **X** ~~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 **within two weeks of the receipt of the complaint with an explanation in cases where the hosting service provider decides not to reinstate the content. A reinstatement of content shall not preclude administrative or judicial measures against the decision of the hosting service provider or of the competent authority**.

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 **or shall provide the content provider a copy of the removal order issued in accordance with Article 4.**

3. The obligation pursuant to paragraphs 1 and 2 shall not apply where the competent authority decides**, considering the proportionality and necessity of such decision,** 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. In such a case, the hosting service provider shall not disclose any information on the removal or disabling of access to terrorist content. **This period can be prolonged once for another six weeks, where justified reasons continue to exist.**

SECTION IV

Cooperation between Competent Authorities, Union Bodies and Hosting Service Providers

Article 12

Capabilities of competent authorities

1. 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.

2. Member States shall ensure that their national competent authorities exercise their tasks in a manner that is objective, non-discriminatory and in full respect of fundamental rights. Competent authorities shall not seek or take instructions from any other body in relation to the exercise of the tasks assigned to them pursuant to Article 17 (1) . This shall not prevent supervision in accordance with national constitutional law.

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 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~~ **X** 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 **and secure** 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 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 **specific** ~~proactive~~ measures pursuant to Article ~~6~~**X**.

4. Where hosting service providers become aware of ~~any evidence of terrorist offences~~ **terrorist content involving an imminent threat to life**, 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~~osting service providers ~~may, in case of doubt,~~ **shall notify the point of contact in the Member State pursuant to Article 17(1a), where they have their main establishment or a legal representative, and also** transmit this information to Europol for appropriate follow up.

5. The competent authorities are encouraged to send copies of the removal orders to Europol allowing Europol to provide an annual report, including an analysis of the types of content subject to removal orders transmitted to the hosting service providers pursuant to this Regulation.

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~~ **expeditious** 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 Article~~s~~ 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[15].~~

15 Moved to Art. 17.

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~~**X** , 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 **which does not have its main establishment within one of the Member States** 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 a~~n~~ **main** 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~~, **reasoned decisions under Article 4a** ~~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**s** 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;~~ **scrutinise removal orders pursuant to Article 4a**

   (c) oversee the implementation of **specific** ~~proactive~~ measures pursuant to Article ~~6~~**X**;

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

1a. Member States shall designate a point of contact within the competent authorities to handle requests for clarification and feedback in relation to removal orders issued by them. Information on the contact point shall be made publicly available.

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*.

2a. By [twelve months after the entry into force of this Regulation] at the latest the Commission shall set up an online register listing all those competent authorities and the designated contact point for each competent authority. The Commission shall publish any modifications regularly.

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), **Article 4a(2), (3) and (4)** (implementation of and feedback on removal orders);

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

(d) Article **X (1), (2), (3), (5) and (6)** ~~6(2) and (4)~~ (**hosting service providers' terms and conditions, obligation to take specific measures, safeguard with regard to the implementation of specific measures**, reports on **specific** ~~proactive~~ measures and the adoption of measures following a decision **under Article X (5)** ~~imposing specific proactive~~ measures);

(e) Article 7 (preservation of data);

(f) Article 8 (transparency **for hosting service providers**);

~~(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 **content** ~~offences~~);

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

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

2. The penalties **pursuant to paragraph 1** ~~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 **deciding whether to impose a penalty and 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 ~~.~~ **;**

(f) **the nature and size of the hosting service providers, in particular for microenterprises or small-sized enterprises within the meaning of Commission Recommendation 2003/361/EC;**

(g) **the degree of fault of the hosting service provider for the breach, taking into account the technical and organisational measures taken by the hosting service provider to comply with the relevant requirements of this Regulation.**

4. Member States shall ensure that a systematic **or persistent** 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 **the necessary** 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 **in the previous calendar year**. 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 **X**~~6~~, including the amount of terrorist content which has been removed or access to it disabled and the corresponding timeframes;

(ba) information about the number of access requests issued by competent authorities regarding content preserved by hosting service providers pursuant to Article 7;

(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~~ [**Two** ~~*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**, the impact of the application of this Regulation on fundamental rights, in particular the freedom of expression and information, the respect for private life and the protection of personal data, and the contribution of this Regulation on the protection of public security**. 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. **The Commission shall also assess the necessity and feasibility of establishing an European Platform on Terrorist Content Online, for facilitating communication and cooperation under this Regulation**.

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*

ANNEX I

REMOVAL ORDER FOR TERRORIST CONTENT (Article 4 of Regulation (EU) xxx)

Under Article 4 of Regulation (EU)….[16] the addressee of the removal order shall remove terrorist content or disable access to it, within one hour from receipt of the removal order from the competent authority.

In accordance with Article 7 of Regulation (EU) ….[17], addressees must preserve content and related data, which has been removed or access to it disabled, for six months or longer upon request from the competent authorities or courts.

The removal order should be sent in one of the languages designated by the addressee pursuant to Article 14(2)

SECTION A:

Issuing Member State:

……..……..

NB: details of issuing authority to be provided at the end (Sections E and F)

Addressee (legal representative)

……..……..

Addressee (contact point)

……..……..

Member State of jurisdiction of addressee: [if different to issuing state]

……..……..

[16] Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (*OJ L* …).

[17] Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (*OJ L* …).

Time and date of issuing the removal order

……..……..

Reference number of the removal order:

……..……..

SECTION B: Content to be removed or access to it disabled within one hour:

A URL and any additional information enabling the identification and exact location of the content referred:

……..……

Reason(s) explaining why the content is considered terrorist content, in accordance with Article 2 (5) of the Regulation (EU) xxx. The content (tick the relevant box(es)):

□ incites, advocates or glorifies the commisison of terrorist offences (Article 2 (5) a)

□ encourages the contribution to terrorist offences (Article 2 (5) b)

□ ~~promotes~~ **solicits** the activities of a terrorist group, encouraging participation in or support of the group (Article 2 (5) c)

□ provides instructions or techniques for committing terrorist offences (Article 2 (5) d)

□ constitutes a threat to commit one of the terrorist offences (Article 2 (5) (e).

Additional information on the reasons why the content is considered terrorist content ~~(optional)~~:

……

……..

…….

SECTION C: Information to content provider

Please note that (tick, if applicable):

□ for reasons of public security, the addressee **must refrain from informing the content provider** whose content is being removed or or to which access has been disabled.

Otherwise: Details of possibilities to contest the removal order in the issuing Member State (which can be passed to the content provider, if requested) under national law; see Section G below:

SECTION D: Informing Member State of jurisdiction

□Tick if the state of jurisidiction of the addressee is other than the issuing Member State:

□ a copy of the removal order is sent to the relevant competent authority of the state of jurisdiction

SECTION E: Details of the authority which issued the removal order

The type of authority which issued this removal order (tick the relevant box):

□ judge, court, or investigating judge

□ law enforcement authority

□ other competent authority→ please complete also Section (F)

Details of the issuing authority and/or its representative certifying the removal order as accurate and correct:

Name of authority:

……..……

Name of its representative:

……..……

Post held (title/grade):

……..……

File No:…..……..……..……..

Address:…….……..……..

Tel. No: (country code) (area/city code) ……..…….

Fax No: (country code) (area/city code) ……..……

Email: ……..……..…….

Date:……..……

Official stamp (if available) and signature[18]: ……...……

[18] A signature may not be necessary if sent through authenticated submission channels.

SECTION F: Contact details for follow-up

Contact details where issuing authority can be reached to receive feedback on time of removal or the disabling of access, or to provide further clarification :

……..…….

Contact details of the authority of the state of jurisdiction of the addressee [if different to the issuing Member State]

……..…….

SECTION G: Information about redress possibilities

Information about competent body or court, deadlines and procedures for contesting the removal order:

Competent body or court to contest the removal order:

…….…….

Deadline for contesting the decision:

Xxx months starting from xxxx

Link to provisions in national legislation:

…….…….

ANNEX II

FEEDBACK FORM FOLLOWING REMOVAL OR DISABLING OF TERRORIST CONTENT (Article 4 (5) of Regulation (EU) xxx)

SECTION A:

Addressee of the removal order :

……..……..

Authority which issued the removal order:

……..……..

File reference of the issuing authority

……..……..

File reference of the addressee:

……..……..

Time and date of receipt of removal order:

……..……..

SECTION B:

The terrorist content/access to terrorist content, subject to the removal order has been (tick the relevant box):

□ removed

□ disabled

Time and date of removal or disabling access ……..

SECTION C: Details of the addressee

Name of the hosting service provider/ legal representative:

……..……..

Member State of main establishment or of establishment of the legal representative:

……..……..

Name of the authorised person:

……..……..

Details of contact point (Email):

…….

Date:

……..……..

ANNEX III

INFORMATION ON THE IMPOSSIBILITY TO EXECUTE THE REMOVAL ORDER

(Article 4 (6) and (7) of Regulation (EU) xxx)

SECTION A:

Addressee of the removal order:

……..……..

Authority which issued the removal order:

……..……..

File reference of the issuing authority:

……..……..

File reference of the addressee:

……..……..

Time and date of receipt of removal order:

……..……..

SECTION B: Reasons for non-execution

(i) The removal order cannot be executed or cannot be executed within the requested deadline for the following reason(s):

- □ *force majeure* or de facto impossibility not attributable to the addressee or the service provider **including for objectively justifiable technical and operational reasons**
- □ the removal order contains manifest errors
- □ the removal order does not contain sufficient information

(ii) Please provide further information as to the reasons for non-execution:

…….

(iii) If the removal order contains manifest errors and/or does not contain sufficient information, please specify which errors and what further information or clarification is required:

…….

SECTION H: Details of the service provider / its legal representative

Name of the service provider/ legal representative:

……..……..

Name of the authorised person:

……..……..

Contact details (Email):

……..……..

Signature:

……..……..

Time and date:

……..……..