REGULATION (EU) 2021/784 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 29 April 2021

on addressing the dissemination of terrorist content online

(Text with EEA relevance)

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 ([2]),

Whereas:

(1) This Regulation aims to ensure the smooth functioning of the digital single market in an open and democratic society, by addressing the misuse of hosting services for terrorist purposes and contributing to public security across the Union. The functioning of the digital single market should be improved by reinforcing legal certainty for hosting service providers and users' trust in the online environment, as well as by strengthening safeguards to the freedom of expression, including the freedom to receive and impart information and ideas in an open and democratic society and the freedom and pluralism of the media.

(2) Regulatory measures to address the dissemination of terrorist content online should be complemented by Member State strategies to address terrorism, including the strengthening of media literacy and critical thinking, the development of 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, deradicalisation initiatives and engagement with affected communities, in order to achieve the sustained prevention of radicalisation in society.

(3) Addressing terrorist content online, which is part of a broader problem of illegal content online, requires a combination of legislative, non-legislative and voluntary measures based on collaboration between authorities and hosting service providers, in a manner that fully respects fundamental rights.

(4) 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, the services of hosting service providers are in certain cases abused by third parties for the purpose of carrying out illegal activities online. Of particular concern is the misuse of those services by terrorist groups and their supporters to disseminate terrorist content online in order to spread their message, to radicalise and recruit followers, and to facilitate and direct terrorist activity.

([1]) OJ C 110, 22.3.2019, p. 67.

([2]) Position of the European Parliament of 17 April 2019 (not yet published in the Official Journal) and position of the Council at first reading of 16 March 2021 (OJ C 135, 16.4.2021, p. 1). Position of the European Parliament of 28 April 2021 (not yet published in the Official Journal).

(5) While not the only factor, the 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, 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, hosting service providers have particular societal responsibilities to protect their services from misuse by terrorists and to help address terrorist content disseminated through their services online, while 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.

(6) 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. Those efforts need to be complemented by a clear legislative framework in order to further reduce the accessibility of terrorist content online and adequately address a rapidly evolving problem. The legislative framework seeks to build on voluntary efforts, which were reinforced by Commission Recommendation (EU) 2018/334 ([3]), and responds to calls made by the European Parliament to strengthen measures to address illegal and harmful content online in line with the horizontal framework established by Directive 2000/31/EC of the European Parliament and of the Council ([4]), as well as by the European Council to improve the detection and removal of content online that incites terrorist acts.

(7) This Regulation should not affect the application of Directive 2000/31/EC. In particular, any measures taken by a hosting service provider in compliance with this Regulation, including any specific measures, should not in themselves lead to that hosting service provider losing the benefit of the liability exemption provided for in that Directive. Moreover, this Regulation does not affect the powers of national authorities and courts to establish the liability of hosting service providers where the conditions set out in that Directive for liability exemption are not met.

(8) In the event of a conflict between this Regulation and Directive 2010/13/EU of the European Parliament and of the Council ([5]) in relation to provisions governing audiovisual media services as defined in point (a) of Article 1(1) of that Directive, Directive 2010/13/EU should prevail. This should leave the obligations under this Regulation, in particular with regard to video-sharing platform providers, unaffected.

(9) This Regulation should set out rules to address the misuse of hosting services for the dissemination of terrorist content online in order to guarantee the smooth functioning of the internal market. Those rules should fully respect the fundamental rights protected in the Union and, in particular, those guaranteed by the Charter of Fundamental Rights of the European Union (the 'Charter').

(10) This Regulation seeks to contribute to the protection of public security while establishing appropriate and robust safeguards to ensure the protection of fundamental rights, including the right to respect for private life, to the protection of personal data, to freedom of expression, including the freedom to receive and impart information, the freedom to conduct a business, and to an effective remedy. Moreover, any discrimination is prohibited. 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 and the freedom and pluralism of the media, which constitute the essential foundations of a pluralist and democratic society and are values on which the Union is founded. Measures affecting the freedom of expression and information should be strictly targeted to address the dissemination of terrorist content online, while respecting 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 measures to address terrorist content online and the protection of freedom of expression and information are not conflicting but complementary and mutually reinforcing goals.

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

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

([5]) Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (OJ L 95, 15.4.2010, p. 1).

(11) In order to provide clarity about the actions that both hosting service providers and competent authorities are to take to address the dissemination of terrorist content online, this Regulation should establish a definition of 'terrorist content' for preventative purposes, consistent with the definitions of relevant offences under Directive (EU) 2017/541 of the European Parliament and of the Council ([6]). Given the need to address the most harmful terrorist propaganda online, that definition should cover material that incites or solicits someone to commit, or to contribute to the commission of, terrorist offences, solicits someone to participate in activities of a terrorist group, or glorifies terrorist activities including by disseminating material depicting a terrorist attack. The definition should also include material that provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, as well as chemical, biological, radiological and nuclear (CBRN) substances, or on other specific methods or techniques, including the selection of targets, for the purpose of committing or contributing to the commission of terrorist offences. Such material includes text, images, sound recordings and videos, as well as live transmissions of terrorist offences, that cause a danger of further such offences being committed. When assessing whether material constitutes terrorist content within the meaning of this Regulation, competent authorities and hosting service providers should take into account factors such as the nature and wording of statements, the context in which the statements were made and their potential to lead to harmful consequences in respect of the security and safety of persons. The fact that the material was produced by, is attributable to or is disseminated on behalf of a person, group or entity included in the Union list of persons, groups and entities involved in terrorist acts and subject to restrictive measures should constitute an important factor in the assessment.

(12) Material disseminated for educational, journalistic, artistic or research purposes or for awareness-raising purposes against terrorist activity should not be considered to be terrorist content. When determining whether the material provided by a content provider constitutes 'terrorist content' as defined in this Regulation, account should be taken, in particular, of the right to freedom of expression and information, including the freedom and pluralism of the media, and the freedom of the arts and sciences. Especially in cases where the content provider holds 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 in accordance with Union law, including the Charter. Furthermore, the expression of radical, polemic or controversial views in the public debate on sensitive political questions should not be considered to be terrorist content.

(13) In order to effectively address the dissemination of terrorist content online, 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 user of the service on request, irrespective of whether the storing and dissemination to the public of such information and material is of a mere technical, automatic and passive nature. 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 storage, such as registries and registrars, as well as providers of domain name systems (DNS), payment or distributed denial of service (DdoS) protection services, should therefore fall outside the scope of this Regulation.

(14) The concept of 'dissemination to the public' should entail the making available of information to a potentially unlimited number of persons, namely making the information easily accessible to users in general, without requiring further action by the content provider, 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, that information 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 point (5) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council ([7]), such as emails or private messaging services, should fall outside the scope of this Regulation. Information should be considered to be stored

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

([7]) Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

and disseminated to the public within the meaning of this Regulation only where such activities are performed upon direct request of the content provider. Consequently, providers of services, such as cloud infrastructure, which are provided at the request of parties other than the content providers and only indirectly benefit the latter, should not be covered by this Regulation. This Regulation should cover, for example, providers of social media, video, image and audio-sharing services, as well as file-sharing services and other cloud services, insofar as those services are used to make the stored information available to the public at the direct request of the content provider. Where a hosting service provider offers several services, this Regulation should apply only to the services that fall within its scope.

(15) Terrorist content is often disseminated to the public through services provided by hosting service providers established in third countries. In order to protect users in the Union and to ensure that all hosting 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 the country of their main establishment. A hosting service provider should be considered offering services in the Union if it enables natural or legal persons in one or more Member States to use its services and has a substantial connection to that Member State or those Member States.

(16) A substantial connection to the Union should exist where the hosting service provider has an establishment in the Union, its services are used by a significant number of users in one or more Member States, or its activities are targeted towards one or more Member States. The targeting of activities towards one or more Member States should be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in the Member State concerned, or the possibility of ordering goods or services from such Member State. Such targeting could also be derived from the availability of an application in the relevant national application store, from providing local advertising or advertising in a language generally used in the Member State concerned, or from the handling of customer relations such as by providing customer service in a language generally used in that Member State. A substantial connection should also be assumed where a hosting service provider directs its activities towards one or more Member States as set out in point (c) of Article 17(1) of Regulation (EU) No 1215/2012 of the European Parliament and of the Council ([8]). The mere accessibility of a hosting service provider's website, of an email address or of other contact details in one or more Member States, taken in isolation, should not be sufficient to constitute a substantial connection. Moreover, the provision of a service with a view to mere compliance with the prohibition of discrimination laid down in Regulation (EU) 2018/302 of the European Parliament and of the Council ([9]) should not, on that ground alone, be considered to constitute a substantial connection to the Union.

(17) The procedure and obligations resulting from removal orders requiring hosting service providers to remove or disable access to terrorist content, following an assessment by the competent authorities, should be harmonised. Given the speed at which terrorist content is disseminated across online services, an obligation should be imposed on hosting service providers to ensure that the terrorist content identified in the removal order is removed or access to it is disabled in all Member States within one hour of receipt of the removal order. Except for in duly justified cases of emergency, the competent authority should provide the hosting service provider with information on procedures and applicable deadlines at least 12 hours in advance of issuing for the first time a removal order to that hosting service provider. Duly justified cases of emergency occur where the removal of or disabling of access to the terrorist content later than one hour after receipt of the removal order would result in serious harm, such as in situations of an imminent threat to the life or physical integrity of a person, or when such content depicts ongoing events resulting in harm to the life or physical integrity of a person. The competent authority should determine whether cases constitute emergency cases and duly justify its decision in the removal order. Where the hosting service provider cannot comply with the removal order within one hour of its receipt, on grounds of *force majeure* or *de facto* impossibility, including for objectively justifiable technical or operational reasons, it should inform the issuing competent authority as soon as possible and comply with the removal order as soon as the situation is resolved.

([8]) Regulation (EU) No 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).

([9]) 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 60 I, 2.3.2018, p. 1).

(18) The removal order should contain a statement of reasons qualifying the material to be removed or access to which is to be disabled as terrorist content and provide sufficient information for the location of that content, by indicating the exact URL and, where necessary, any other additional information, such as a screenshot of the content in question. That statement of reasons should allow the hosting service provider and, ultimately, the content provider to effectively exercise their right to judicial redress. The reasons provided should not imply the disclosure of sensitive information which could jeopardise ongoing investigations.

(19) The competent authority should submit the removal order directly to the contact point designated or established by the hosting service provider for the purposes of this Regulation by any electronic means capable of producing a written record under conditions that allow the hosting service provider to establish the authenticity of the order, including the accuracy of the date and the time of sending and receipt thereof, such as by secured email or platforms or other secured channels, including those made available by the hosting service provider, in accordance with Union law on the protection of personal data. It should be possible for that requirement to be met through the use of, inter alia, qualified electronic registered delivery services as provided for by Regulation (EU) No 910/2014 of the European Parliament and of the Council ([10]). Where the hosting service provider's main establishment is or its legal representative resides or is established in a Member State other than that of the issuing competent authority, a copy of the removal order should be submitted simultaneously to the competent authority of that Member State.

(20) It should be possible for the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established to scrutinise the removal order issued by competent authorities of another Member State to determine whether it seriously or manifestly infringes this Regulation or the fundamental rights enshrined in the Charter. Both the content provider and the hosting service provider should have the right to request such scrutiny by the competent authority in the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established. Where such a request is made, that competent authority should adopt a decision on whether the removal order comprises such an infringement. Where that decision finds such an infringement, the removal order should cease to have legal effects. The scrutiny should be carried out swiftly so as to ensure that erroneously removed or disabled content is reinstated as soon as possible.

(21) 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 those provisions in a diligent, transparent, proportionate and non-discriminatory manner.

(22) Given the scale of the problem and the speed necessary to effectively identify and remove terrorist content, effective and proportionate specific measures are an essential element in addressing terrorist content online. With a view to reducing the accessibility of terrorist content on their services, hosting service providers exposed to terrorist content should put in place specific measures taking into account the risks and level of exposure to terrorist content as well as the effects on the rights of third parties and the public interest to information. Hosting service providers should determine what appropriate, effective and proportionate specific measure should be put in place to identify and remove terrorist content. Specific measures could 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.

(23) When putting in place 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 Charter are preserved. In addition to any requirement laid down in the law, including legislation on the protection of personal data, hosting service providers should act with due diligence and implement safeguards, where appropriate, including human oversight and verifications, to avoid any unintended or erroneous decision leading to the removal of or disabling of access to content that is not terrorist content.

([10]) 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).

(24) The hosting service provider should report to the competent authority on the specific measures in place in order to allow that authority to determine whether the measures are effective and proportionate and whether, if automated means are used, the hosting service provider has the necessary capacity 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 issued to the hosting service provider, the size and economic capacity of the hosting service provider and the impact of its services in disseminating terrorist content, for example on the basis of the number of users in the Union, as well as the safeguards put in place to address the misuse of its services for the dissemination of terrorist content online.

(25) Where the competent authority considers that the specific measures put in place are insufficient to address the risks, it should be able to require the adoption of additional appropriate, effective and proportionate specific measures. The requirement to implement such additional specific measures should not lead to a general obligation to monitor or to engage in active fact-finding within the meaning of Article 15(1) of Directive 2000/31/EC or to an obligation to use automated tools. However, it should be possible for hosting service providers to use automated tools if they consider this to be appropriate and necessary to effectively address the misuse of their services for the dissemination of terrorist content.

(26) The obligation on hosting service providers to preserve removed content and related data should be laid down for specific purposes and limited to the period necessary. There is a 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 terrorist content in question. Related data can include data such as subscriber data, in particular data pertaining to the identity of the content provider, as well as access data, including data about the date and time of use by the content provider and 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.

(27) The obligation to preserve the content for administrative or judicial review proceedings is necessary and justified in view of the need to ensure that effective remedies are in place for content providers whose content has been removed or access to which has been disabled, as well as to ensure the reinstatement of that content, depending on the outcome of those proceedings. The obligation to preserve material for investigative or prosecutorial purposes is justified and necessary in view of the value the material could have for the purpose of disrupting or preventing terrorist activity. Therefore, the preservation of removed terrorist content for the purposes of prevention, detection, investigation and prosecution of terrorist offences should also be considered to be justified. The terrorist content and the related data should be stored only for the period necessary to allow the law enforcement authorities to check that terrorist content and decide whether it would be needed for those purposes. For the purposes of the prevention, detection, investigation and prosecution of terrorist offences, the required preservation of data should be limited to data that are likely to have a link with terrorist offences, and could therefore contribute to prosecuting terrorist offences or to preventing serious risks to public security. Where hosting service providers remove or disable access to material, in particular through their own specific measures, they should inform the competent authorities promptly of content that contains information involving an imminent threat to life or a suspected terrorist offence.

(28) To ensure proportionality, the period of preservation should be limited to six months to allow content providers sufficient time to initiate administrative or judicial review proceedings and to enable access by law enforcement authorities to relevant data for the investigation and prosecution of terrorist offences. However, upon the request of the competent authority or court, it should be possible to extend that period for as long as necessary in cases where those proceedings are initiated but not finalised within that six-month period. The duration of the period of preservation should be sufficient to allow law enforcement authorities to preserve the necessary material in relation to investigations and prosecutions, while ensuring the balance with the fundamental rights.

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

(30) The 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 or were required to take action pursuant to this Regulation in a given calendar year should make publicly available annual transparency reports containing information about action taken in relation to the identification and removal of terrorist content.

(31) The competent authorities should publish annual transparency reports containing information on the number of removal orders, the number of cases where an order was not executed, the number of decisions concerning specific measures, the number of cases subject to administrative or judicial review proceedings and the number of decisions imposing penalties.

(32) The right to an effective remedy is enshrined in Article 19 of the Treaty on European Union (TEU) and in Article 47 of the Charter. Each natural or legal person has the right to an effective 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. That right should include, in particular, the possibility for hosting service providers and content providers to effectively challenge the removal orders or any decisions resulting from the scrutiny of removal orders under this Regulation before a court of the Member State whose competent authority issued the removal order or took the decision, as well as for hosting service providers to effectively challenge a decision relating to specific measures or penalties before a court of the Member State whose competent authority took that decision.

(33) Complaint procedures constitute a necessary safeguard against the erroneous removal of or disabling of access to content online where such content is 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 expeditiously and in full transparency towards the content provider. The requirement for the hosting service provider to reinstate content that has been removed or access to which has been disabled in error should not affect the possibility for the hosting service provider to enforce its own terms and conditions.

(34) Effective legal protection in accordance with Article 19 TEU and Article 47 of the Charter requires that content providers are able to ascertain the reasons upon which the content they provide has been removed or access to which has been disabled. For that purpose, the hosting service provider should make available to the content provider information for challenging the removal or the disabling. Depending on the circumstances, hosting service providers could replace content which has been removed or access to which has been disabled with a message indicating that the content has been removed or access to it has been disabled in accordance with this Regulation. Further information about the reasons for the removal or disabling as well as the remedies for the removal or disabling should be provided upon request of the content provider. Where the competent authorities decide that for reasons of public security, including in the context of an investigation, it is inappropriate or counterproductive to directly notify the content provider of the removal or disabling, they should inform the hosting service provider accordingly.

(35) For the purposes of this Regulation, Member States should designate competent authorities. This should not necessarily imply the establishment of a new authority and it should be possible to entrust an existing body with the functions provided for in this Regulation. This Regulation should require the designation of authorities competent for issuing removal orders, scrutinising removal orders, overseeing specific measures and imposing penalties, while it should be possible for each Member State to decide on the number of competent authorities to be designated and whether they are administrative, law enforcement or judicial. Member States should ensure that the competent authorities fulfil 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 under this Regulation. This should not prevent supervision in accordance with national constitutional law. Member States should communicate the competent authorities designated under this Regulation to the Commission, which should publish online a register listing the competent authorities. That online register should be easily accessible to facilitate the swift verification of the authenticity of removal orders by the hosting service providers.

(36) In order to avoid duplication of effort and possible interferences with investigations and to minimise the burden to the hosting service providers affected, the competent authorities should exchange information, coordinate and cooperate with each other and, where appropriate, with Europol, before issuing removal orders. When deciding whether to issue a removal order, the competent authority should give due consideration to any notification of an interference with an investigative interest (deconfliction). Where a competent authority is informed by a competent authority of another Member State of an existing removal order, it should not issue a removal order concerning the same subject matter. In implementing the provisions of this Regulation, Europol could provide support in line with its current mandate and existing legal framework.

(37) In order to ensure the effective and sufficiently coherent implementation of specific measures taken by hosting service providers, competent authorities should coordinate and cooperate with each other with regard to the exchanges with hosting service providers as to removal orders and the identification, implementation and assessment of specific measures. Coordination and cooperation are also needed in relation to other measures to implement this Regulation, including with respect to the adoption of rules on penalties and the imposition of penalties. The Commission should facilitate such coordination and cooperation.

(38) It is essential that the competent authority of the Member State responsible for imposing penalties is fully informed of the issuing of removal orders and of the subsequent exchanges between the hosting service provider and the competent authorities 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.

(39) To facilitate the swift exchanges between competent authorities as well as with hosting service providers, and to avoid duplication of effort, Member States should be encouraged to make use of the dedicated tools developed by Europol, such as the current internet Referral Management application or its successors.

(40) Referrals by Member States and Europol have proven to be an effective and swift means of increasing hosting service providers' awareness of specific content available through their services and enabling them to take swift action. Such referrals, which are a mechanism for alerting hosting service providers of information that could be considered to be terrorist content for the provider's voluntary consideration of the compatibility of that content with its own terms and conditions, should remain available in addition to removal orders. The final decision on whether to remove the content because it is incompatible with its terms and conditions remains with the hosting service provider. This Regulation should not affect the mandate of Europol as laid down in Regulation (EU) 2016/794 of the European Parliament and of the Council ([11]). 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 online.

(41) Given the particular serious consequences of certain terrorist content online, hosting service providers should promptly inform the relevant authorities in the Member State concerned or the competent authorities of the Member State where they are established or have a legal representative of terrorist content involving an imminent threat to life or a suspected terrorist offence. In order to ensure proportionality, that obligation should be limited to terrorist offences as defined in Article 3(1) of Directive (EU) 2017/541. That obligation to inform should not imply an obligation on hosting service providers to actively seek any evidence of such imminent threat to life or a suspected terrorist offence. The Member State concerned should be understood to be the Member State with jurisdiction over the investigation and prosecution of those terrorist offences based on the nationality of the offender or of the potential victim of the offence or the target location of the terrorist act. In the case of doubt, hosting service providers should submit the information to Europol, which should provide the relevant follow-up action in accordance with its mandate, including by forwarding that information to the relevant national authorities. The competent authorities of the Member States should be allowed to use such information to take investigatory measures available under Union or national law.

([11]) 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).

(42) Hosting service providers should designate or establish contact points to facilitate the expeditious handling of removal orders. The contact point should serve only for operational purposes. The contact point should consist of any dedicated means, in-house or outsourced, allowing for the electronic submission of removal orders and of technical or personal means allowing for the expeditious processing thereof. It is not necessary that the contact point be located in the Union. The hosting service provider should be free to make use of an existing contact point for the purpose of this Regulation, provided that the contact point is able to fulfil the functions provided for in this Regulation. With a view to ensuring that terrorist content is removed or that access thereto is disabled within one hour of receipt of a removal order, the contact points of hosting service providers exposed to terrorist content should be accessible at any time. The information on the contact point should include information about the language in which it 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 institutions in which their terms and conditions are available.

(43) In the absence of a general requirement for hosting 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 its legal representative resides or is established. 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. With regard to a hosting service provider which has no establishment in the Union and does not designate a legal representative, any Member State should, nevertheless, have jurisdiction and therefore be able to impose penalties, provided that the principle of *ne bis in idem* is respected.

(44) Hosting service providers that are not established in the Union should designate in writing a legal representative in order to ensure compliance with and the enforcement of the obligations under this Regulation. It should be possible for hosting service providers to designate, for the purposes of this Regulation, a legal representative already designated for other purposes, provided that that legal representative is able to fulfil the functions provided for in this Regulation. The legal representative should be empowered to act on behalf of the hosting service provider.

(45) Penalties are necessary to ensure the effective implementation of this Regulation by hosting service providers. Member States should adopt rules on penalties, which can be of an administrative or criminal nature, as well as, where appropriate, fining guidelines. Non-compliance in individual cases could be subject to penalties while respecting the principles of *ne bis in idem* and of proportionality and ensuring that such penalties take account of systematic failure. Penalties could take different forms, including formal warnings in the case of minor infringements or financial penalties in relation to more severe or systematic infringements. Particularly severe penalties should be imposed in the event that the hosting service provider systematically or persistently fails to remove or disable access to terrorist content within one hour of receipt of a removal order. In order to ensure legal certainty, this Regulation should set out which infringements are subject to penalties and which circumstances are relevant for assessing the type and level of such penalties. When determining whether to impose financial penalties, due account should be taken of the financial resources of the hosting service provider. Moreover, the competent authority should take into account whether the hosting service provider is a start-up or a micro, small or medium-sized enterprise as defined in Commission Recommendation 2003/361/EC ([12]). 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 be taken into account. Member States should ensure that penalties imposed for the infringement of this Regulation do not encourage the removal of material which is not terrorist content.

(46) The use of standardised templates facilitates cooperation and the exchange of information between competent authorities and hosting service providers, allowing them to communicate more quickly and effectively. It is particularly important to ensure expeditious action following the receipt of a removal order. Templates reduce translation costs and contribute to a higher standard of the process. Feedback templates allow for a standardised exchange of information and are particularly important where hosting service providers are unable to comply with removal orders. 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.

([12]) Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

(47) 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 in respect of amending the annexes to 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 carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([13]). 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.

(48) Member States should collect information on the implementation of this Regulation. It should be possible for Member States to make use of the hosting service providers' transparency reports and complement them, where necessary, with more detailed information, such as their own transparency reports pursuant to 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 implementation of this Regulation.

(49) 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 within three years of the date of its entry into force. The evaluation should be based on the criteria of efficiency, necessity, effectiveness, proportionality, relevance, coherence and Union added value. It should assess the functioning of the different operational and technical measures provided for by this Regulation, including the effectiveness of measures to enhance the detection, identification and removal of terrorist content online, the effectiveness of safeguard mechanisms as well as the impacts on potentially affected fundamental rights, such as the freedom of expression and information, including the freedom and pluralism of the media, the freedom to conduct a business, the right to private life and the protection of personal data. The Commission should also assess the impact on potentially affected interests of third parties.

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

HAVE ADOPTED THIS REGULATION:

SECTION I

GENERAL PROVISIONS

Article 1

Subject matter and scope

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

(a) reasonable and proportionate duties of care to be applied by hosting service providers in order to address the dissemination to the public of terrorist content through their services and ensure, where necessary, the expeditious removal of or disabling of access to such content;

([13]) OJ L 123, 12.5.2016, p. 1.

(b) the 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, in order to:

(i) identify and ensure the expeditious removal of terrorist content by hosting service providers; and

(ii) facilitate cooperation among the competent authorities of Member States, hosting service providers and, where appropriate, Europol.

2. This Regulation applies to hosting service providers offering services in the Union, irrespective of their place of main establishment, insofar as they disseminate information to the public.

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

4. This Regulation shall not have the effect of modifying the obligation to respect the rights, freedoms and principles referred to in Article 6 TEU and shall apply without prejudice to fundamental principles relating to freedom of expression and information, including freedom and pluralism of the media.

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

Article 2

Definitions

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

(1) 'hosting service provider' means a provider of services as defined in point (b) of Article 1 of Directive (EU) 2015/1535 of the European Parliament and of the Council ([14]), consisting of the storage of information provided by and at the request of a content provider;

(2) 'content provider' means a user that has provided information that is, or that has been, stored and disseminated to the public by a hosting service provider;

(3) 'dissemination to the public' means the making available of information, at the request of a content provider, to a potentially unlimited number of persons;

(4) 'offering services in the Union' means enabling natural or legal persons in one or more Member States to use the services of a hosting service provider which has a substantial connection to that Member State or those Member States;

(5) 'substantial connection' means the connection of a hosting service provider with one or more Member States resulting either from its establishment in the Union or from specific factual criteria, such as:

(a) having a significant number of users of its services in one or more Member States; or

(b) the targeting of its activities to one or more Member States;

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

([14]) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

(7) 'terrorist content' means one or more of the following types of material, namely material that:

(a) incites 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 of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed;

(b) solicits a person or a group of persons to commit or contribute to the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;

(c) solicits a person or a group of persons to participate in the activities of a terrorist group, within the meaning of point (b) of Article 4 of Directive (EU) 2017/541;

(d) provides instruction 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) constitutes a threat to commit one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;

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

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

SECTION II

MEASURES TO ADDRESS THE DISSEMINATION OF TERRORIST CONTENT ONLINE

Article 3

Removal orders

1. The competent authority of each Member State shall have the power to issue a removal order requiring hosting service providers to remove terrorist content or to disable access to terrorist content in all Member States.

2. Where a competent authority has not previously issued a removal order to a hosting service provider, it shall provide that hosting service provider with information on the applicable procedures and deadlines, at least 12 hours before issuing the removal order.

The first subparagraph shall not apply in duly justified cases of emergency.

3. Hosting service providers shall remove terrorist content or disable access to terrorist content in all Member States as soon as possible and in any event within one hour of receipt of the removal order.

4. Competent authorities shall issue removal orders using the template set out in Annex I. Removal orders shall contain the following elements:

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

(b) a sufficiently detailed statement of reasons explaining why the content is considered to be terrorist content, and a reference to the relevant type of material referred to in point (7) of Article 2;

(c) an exact uniform resource locator (URL) and, where necessary, additional information for the identification of the terrorist content;

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

(e) the date, time stamp and electronic signature of the competent authority issuing the removal order;

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

(g) where necessary and proportionate, the decision not to disclose information about the removal of or disabling of access to terrorist content in accordance with Article 11(3).

5. The competent authority shall address the removal order to the main establishment of the hosting service provider or to its legal representative designated in accordance with Article 17.

That competent authority shall transmit the removal order to the contact point referred to in Article 15(1) by electronic means capable of producing a written record under conditions that allow to establish the authentication of the sender, including the accuracy of the date and the time of sending and receipt of the order.

6. The hosting service provider shall, without undue delay, inform the competent authority, using the template set out in Annex II, of the removal of the terrorist content or the disabling of access to the terrorist content in all Member States, indicating, in particular, the time of that removal or disabling.

7. If the hosting service provider cannot comply with the removal order on grounds of *force majeure* or *de facto* impossibility not attributable to the hosting service provider, including for objectively justifiable technical or operational reasons, it shall, without undue delay, inform the competent authority that issued the removal order of those grounds, using the template set out in Annex III.

The deadline set out in paragraph 3 shall start to run as soon as the grounds referred to in the first subparagraph of this paragraph have ceased to exist.

8. If the hosting service provider cannot comply with the removal order because it contains manifest errors or does not contain sufficient information for its execution, it shall, without undue delay, inform the competent authority that issued the removal order and request the necessary clarification, using the template set out in Annex III.

The deadline set out in paragraph 3 shall start to run as soon as the hosting service provider has received the necessary clarification.

9. A removal order shall become final upon the expiry of the deadline for appeal where no appeal has been lodged in accordance with national law or upon confirmation following an appeal.

When the removal order becomes final, the competent authority that issued the removal order shall inform the competent authority referred to in point (c) of Article 12(1) of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established of that fact.

Article 4

Procedure for cross-border removal orders

1. Subject to Article 3, where the hosting service provider does not have its main establishment or legal representative in the Member State of the competent authority that issued the removal order, that authority shall, simultaneously, 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 where its legal representative resides or is established.

2. Where a hosting service provider receives a removal order as referred to in this Article, it shall take the measures provided for in Article 3 and take the necessary measures to be able to reinstate the content or access thereto, in accordance with paragraph 7 of this Article.

3. The competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established may, on its own initiative, within 72 hours of receiving the copy of the removal order in accordance with paragraph 1, scrutinise the removal order to determine whether it seriously or manifestly infringes this Regulation or the fundamental rights and freedoms guaranteed by the Charter.

Where it finds an infringement, it shall, within the same period, adopt a reasoned decision to that effect.

4. Hosting service providers and content providers shall have the right to submit, within 48 hours of receiving either a removal order or information pursuant to Article 11(2), a reasoned request to the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established to scrutinise the removal order as referred to in the first subparagraph of paragraph 3 of this Article.

The competent authority shall, within 72 hours of receiving the request, adopt a reasoned decision following its scrutiny of the removal order, setting out its findings as to whether there is an infringement.

5. The competent authority shall, before adopting a decision pursuant to the second subparagraph of paragraph 3 or a decision finding an infringement pursuant to the second subparagraph of paragraph 4, inform the competent authority that issued the removal order of its intention to adopt the decision and of its reasons for doing so.

6. Where the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established adopts a reasoned decision in accordance with paragraph 3 or 4 of this Article, it shall, without delay, communicate that decision to the competent authority that issued the removal order, the hosting service provider, the content provider who requested the scrutiny pursuant to paragraph 4 of this Article and, in accordance with Article 14, Europol. Where the decision finds an infringement pursuant to paragraph 3 or 4 of this Article, the removal order shall cease to have legal effects.

7. Upon receiving a decision finding an infringement communicated in accordance with paragraph 6, the hosting service provider concerned shall immediately reinstate the content or access thereto, without prejudice to the possibility to enforce its terms and conditions in accordance with Union and national law.

Article 5

Specific measures

1. A hosting service provider exposed to terrorist content as referred to in paragraph 4 shall, where applicable, include in its terms and conditions and apply provisions to address the misuse of its services for the dissemination to the public of terrorist content.

It shall do so in a diligent, proportionate and non-discriminatory manner, with due regard, in all circumstances, to the fundamental rights of the users and taking into account, in particular, the fundamental importance of the freedom of expression and information in an open and democratic society, with a view to avoiding the removal of material which is not terrorist content.

2. A hosting service provider exposed to terrorist content as referred to in paragraph 4 shall take specific measures to protect its 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. Such 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 user moderation;

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

3. Specific measures shall meet all of the following requirements:

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

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

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

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

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

4. A hosting service provider is exposed to terrorist content where the competent authority of the Member State of its main establishment or where its legal representative resides or is established has:

(a) taken a decision, on the basis of objective factors, such as the hosting service provider having received two or more final removal orders in the previous 12 months, finding that the hosting service provider is exposed to terrorist content; and

(b) notified the decision referred to in point (a) to the hosting service provider.

5. After having received a decision as referred to in paragraph 4 or, where relevant, paragraph 6, a hosting service provider shall report to the competent authority on the specific measures that it has taken and that it intends to take in order to comply with paragraphs 2 and 3. It shall do so within three months of receipt of the decision and on an annual basis thereafter. That obligation shall cease once the competent authority has decided, upon request pursuant to paragraph 7, that the hosting service provider is no longer exposed to terrorist content.

6. Where, based on the reports referred to in paragraph 5 and, where relevant, any other objective factors, the competent authority considers that the specific measures taken do not comply with paragraphs 2 and 3, that competent authority shall address a decision to the hosting service provider requiring it to take the necessary measures so as to ensure that paragraphs 2 and 3 are complied with.

The hosting service provider may choose the type of specific measures to take.

7. A hosting service provider may, at any time, request the competent authority to review and, where appropriate, amend or revoke a decision as referred to in paragraph 4 or 6.

The competent authority shall, within three months of receipt of the request, adopt a reasoned decision on the request based on objective factors and notify the hosting service provider of that decision.

8. Any requirement to take specific measures shall be without prejudice to Article 15(1) of Directive 2000/31/EC and shall entail neither a general obligation for hosting services providers to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

Any requirement to take specific measures shall not include an obligation to use automated tools by the hosting service provider.

Article 6

Preservation of content and related data

1. Hosting service providers shall preserve terrorist content which has been removed or access to which has been disabled as a result of a removal order, or of specific measures pursuant to Article 3 or 5, as well as any related data removed as a consequence of the removal of such terrorist content, which are necessary for:

(a) administrative or judicial review proceedings or complaint-handling under Article 10 against a decision to remove or disable access to terrorist content and related data; or

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

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

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

Those technical and organisational safeguards shall ensure that the terrorist content and related data preserved are accessed and processed only 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 7

Transparency obligations for hosting service providers

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

2. A hosting service provider that has taken action to address the dissemination of terrorist content or has been required to take action pursuant to this Regulation in a given calendar year, shall make publicly available a transparency report on those actions for that year. It shall publish that report before 1 March of the following year.

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

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

(b) information about the hosting service provider's measures to address the reappearance online of material which has previously been removed or to which access has been disabled because it was considered to be terrorist content, in particular where automated tools have been used;

(c) the number of items of terrorist content removed or to which access has been disabled following removal orders or specific measures, and the number of removal orders where the content has not been removed or access to which has not been disabled pursuant to the first subparagraph of Article 3(7) and the first subparagraph of Article 3(8), together with the grounds therefor;

(d) the number and the outcome of complaints handled by the hosting service provider in accordance with Article 10;

(e) the number and the outcome of administrative or judicial review proceedings brought by the hosting service provider;

(f) the number of cases in which the hosting service provider was required to reinstate content or access thereto as a result of administrative or judicial review proceedings;

(g) the number of cases in which the hosting service provider reinstated content or access thereto following a complaint by the content provider.

Article 8

Competent authorities' transparency reports

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

(a) the number of removal orders issued under Article 3, specifying the number of removal orders subject to Article 4(1), the number of removal orders scrutinised under Article 4, and information on the implementation of those removal orders by the hosting service providers concerned, including the number of cases in which terrorist content was removed or access thereto was disabled and the number of cases in which terrorist content was not removed or access thereto was not disabled;

(b) the number of decisions taken in accordance with Article 5(4), (6) or (7), and information on the implementation of those decisions by hosting service providers, including a description of the specific measures;

(c) the number of cases in which removal orders and decisions taken in accordance with Article 5(4) and (6) were subject to administrative or judicial review proceedings and information on the outcome of the relevant proceedings;

(d) the number of decisions imposing penalties pursuant to Article 18, and a description of the type of penalty imposed.

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

Article 9

Remedies

1. Hosting service providers that have received a removal order issued pursuant to Article 3(1) or a decision pursuant to Article 4(4) or to Article 5(4), (6) or (7), shall have a right to an effective remedy. That right shall include the right to challenge such a removal order before the courts of the Member State of the competent authority that issued the removal order and the right to challenge the decision pursuant to Article 4(4) or to Article 5(4), (6) or (7), before the courts of the Member State of the competent authority that took the 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. That right shall include the right to challenge a removal order issued pursuant to Article 3(1) before the courts of the Member State of the competent authority that issued the removal order and the right to challenge a decision pursuant to Article 4(4) before the courts of the Member State of the competent authority that took the decision.

3. Member States shall put in place effective procedures for exercising the rights referred to in this Article.

Article 10

Complaint mechanisms

1. Each hosting service provider shall establish an effective and accessible mechanism allowing content providers where their content has been removed or access thereto has been disabled as a result of specific measures pursuant to Article 5 to submit a complaint concerning that removal or disabling, requesting the reinstatement of the content or of access thereto.

2. Each hosting service provider shall expeditiously examine all complaints that it receives through the mechanism referred to in paragraph 1 and reinstate the content or access thereto, without undue delay, where its removal or disabling of access thereto was unjustified. It shall inform the complainant of the outcome of the complaint within two weeks of the receipt thereof.

Where the complaint is rejected, the hosting service provider shall provide the complainant with the reasons for its decision.

A reinstatement of content or of access thereto shall not preclude administrative or judicial review proceedings challenging the decision of the hosting service provider or of the competent authority.

Article 11

Information to content providers

1. Where a hosting service provider removes or disables access to terrorist content, it shall make available to the content provider information on such removal or disabling.

2. Upon request of the content provider, the hosting service provider shall either inform the content provider of the reasons for the removal or disabling and its rights to challenge the removal order or provide the content provider with a copy of the removal order.

3. The obligation pursuant to paragraphs 1 and 2 shall not apply where the competent authority issuing the removal order decides that it is necessary and proportionate that there 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 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.

That competent authority may extend that period by a further six weeks, where such non-disclosure continues to be justified.

SECTION IV

COMPETENT AUTHORITIES AND COOPERATION

Article 12

Designation of competent authorities

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

(a) issue removal orders pursuant to Article 3;

(b) scrutinise removal orders pursuant to Article 4;

(c) oversee the implementation of specific measures pursuant to Article 5;

(d) impose penalties pursuant to Article 18.

2. Each Member State shall ensure that a contact point is designated or established within the competent authority referred to in point (a) of paragraph 1 to handle requests for clarification and feedback in relation to removal orders issued by that competent authority.

Member States shall ensure that the information on the contact point is made publicly available.

3. By 7 June 2022, Member States shall notify the Commission of the competent authority or authorities referred to in paragraph 1 and any modification thereof. The Commission shall publish the notification and any modification thereto in the *Official Journal of the European Union*.

4. By 7 June 2022, the Commission shall set up an online register listing the competent authorities referred to in paragraph 1 and the contact point designated or established pursuant to paragraph 2 for each competent authority. The Commission shall publish any modification thereto regularly.

Article 13

Competent authorities

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

2. Member States shall ensure that their competent authorities carry out their tasks under this Regulation in an objective and non-discriminatory manner while fully respecting fundamental rights. Competent authorities shall not seek or take instructions from any other body in relation to the carrying out of their tasks under Article 12(1).

The first subparagraph shall not prevent supervision in accordance with national constitutional law.

Article 14

Cooperation between hosting service providers, competent authorities and Europol

1. Competent authorities shall exchange information, coordinate and cooperate with each other and, where appropriate, with Europol, with regard to removal orders, in particular to avoid duplication of effort, enhance coordination and avoid interference with investigations in different Member States.

2. Competent authorities of Member States shall exchange information, coordinate and cooperate with the competent authorities referred to in points (c) and (d) of Article 12(1) with regard to specific measures taken pursuant to Article 5 and penalties imposed pursuant to Article 18. Member States shall ensure that the competent authorities referred to in points (c) and (d) of Article 12(1) are in possession of all the relevant information.

3. For the purposes of paragraph 1, Member States shall provide for the appropriate and secure communication channels or mechanisms to ensure that the relevant information is exchanged in a timely manner.

4. For the effective implementation of this Regulation as well as to avoid duplication of effort, Member States and hosting service providers may make use of dedicated tools, including those established by Europol, to facilitate in particular:

(a) the processing and feedback relating to removal orders pursuant to Article 3; and

(b) cooperation with a view to identifying and implementing specific measures pursuant to Article 5.

5. Where hosting service providers become aware of terrorist content involving an imminent threat to life, they shall promptly inform authorities competent for the investigation and prosecution of criminal offences in the Member States concerned. Where it is impossible to identify the Member States concerned, the hosting service providers shall notify the contact point pursuant to Article 12(2) in the Member State where they have their main establishment or where their legal representative resides or is established, and transmit information concerning that terrorist content to Europol for appropriate follow-up.

6. The competent authorities are encouraged to send copies of the removal orders to Europol to allow it to provide an annual report that includes an analysis of the types of terrorist content subject to an order to remove it or to disable access thereto pursuant to this Regulation.

Article 15

Hosting service providers' contact points

1. Each hosting service provider shall designate or establish a contact point for the receipt of removal orders by electronic means and their expeditious processing pursuant to Articles 3 and 4. The hosting service provider shall ensure that information about the contact point is made publicly available.

2. The information referred to in paragraph 1 of this Article shall specify the official languages of the Union institutions referred to in Regulation 1/58 ([15]) in which the contact point can be addressed and in which further exchanges in relation to removal orders pursuant to Article 3 are to take place. Those languages shall include at least one of the official languages of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established.

SECTION V

IMPLEMENTATION AND ENFORCEMENT

Article 16

Jurisdiction

1. The Member State of the main establishment of the hosting service provider shall have jurisdiction for the purposes of Articles 5, 18 and 21. A hosting service provider which does not have its main establishment within the Union shall be deemed to be under the jurisdiction of the Member State where its legal representative resides or is established.

2. Where a hosting service provider which does not have its main establishment in the Union fails to designate a legal representative, all Member States shall have jurisdiction.

3. Where a competent authority of a Member State exercises jurisdiction pursuant to paragraph 2, it shall inform the competent authorities of all other Member States.

Article 17

Legal representative

1. A hosting service provider which does not have its main establishment in the Union shall designate, in writing, a natural or legal person as its legal representative in the Union for the purpose of the receipt of, compliance with and the enforcement of removal orders and decisions issued by the competent authorities.

2. The hosting service provider shall provide its legal representative with the necessary powers and resources to comply with those removal orders and decisions and to cooperate with the competent authorities.

The legal representative shall reside or be established in one of the Member States where the hosting service provider offers its services.

3. The legal representative may be held liable for infringements of this Regulation, without prejudice to any liability of or legal actions against the hosting service provider.

4. The hosting service provider shall notify the competent authority referred to in point (d) of Article 12(1) of the Member State where its legal representative resides or is established of the designation.

The hosting service provider shall make the information about the legal representative publicly available.

SECTION VI

FINAL PROVISIONS

Article 18

Penalties

1. Member States shall lay down the rules on penalties applicable to infringements of this Regulation by hosting service providers and shall take all measures necessary to ensure that they are implemented. Such penalties shall be limited to addressing infringements of Article 3(3) and (6), Article 4(2) and (7), Article 5(1), (2), (3), (5) and (6), Articles 6, 7, 10 and 11, Article 14(5), Article 15(1) and Article 17.

([15]) Regulation No 1 determining the languages to be used by the European Economic Community (OJ 17, 6.10.1958, p. 385).

The penalties referred to in the first subparagraph shall be effective, proportionate and dissuasive. Member States shall, by 7 June 2022, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

2. Member States shall ensure that the competent authorities, when deciding whether to impose a penalty and when determining the type and level of penalty, take into account all relevant circumstances, including:

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

(b) whether the infringement was intentional or negligent;

(c) previous infringements by the hosting service provider;

(d) the financial strength of the hosting service provider;

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

(f) the nature and size of the hosting service provider, in particular whether it is a micro, small or medium-sized enterprise;

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

3. Member States shall ensure that a systematic or persistent failure to comply with obligations pursuant to Article 3(3) is subject to financial penalties of up to 4 % of the hosting service provider's global turnover of the preceding business year.

Article 19

Technical requirements and amendments to the annexes

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 delegated acts in accordance with Article 20 to amend the annexes in order to effectively address a possible need for improvements regarding the content of templates for removal orders and to provide information on the impossibility to execute removal orders.

Article 20

Exercise of the 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 7 June 2022.

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 of 13 April 2016 on Better Law-Making.

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 by 31 March of every year information about the actions they have taken in accordance with this Regulation in the previous calendar year. That information shall include:

(a) the number of removal orders issued and the number of items of terrorist content which have been removed or access to which has been disabled and the speed of the removal or disabling;

(b) the specific measures taken pursuant to Article 5, including the number of items of terrorist content which have been removed or access to which has been disabled and the speed of the removal or disabling;

(c) the number of access requests issued by competent authorities regarding content preserved by hosting service providers pursuant to Article 6;

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

(e) the number of administrative or judicial review proceedings initiated and decisions taken by the competent authority in accordance with national law.

2. By 7 June 2023, 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 are 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 7 June 2023, the Commission shall submit a report on the application of this Regulation to the European Parliament and to the Council. That report shall include information on monitoring under Article 21 and information resulting from the transparency obligations under Article 8. Member States shall provide the Commission with the information necessary for the drafting of the report.

Article 23

Evaluation

By 7 June 2024, the Commission shall carry out an evaluation of this Regulation and submit a report to the European Parliament and to the Council on its application including:

(a) the functioning and effectiveness of the safeguard mechanisms, in particular those provided for in Article 4(4), Article 6(3) and Articles 7 to 11;

(b) 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

(c) the contribution of this Regulation to 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 drafting of the report.

The Commission shall also assess the necessity and feasibility of establishing a European platform on terrorist content online for facilitating communication and cooperation under this Regulation.

Article 24

Entry into force and application

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 7 June 2022.

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

Done at Brussels, 29 April 2021.

For the European Parliament	*For the Council*
The President	*The President*
D.M. SASSOLI	A.P. ZACARIAS

ANNEX I

REMOVAL ORDER

(Article 3 of Regulation (EU) 2021/784 of the European Parliament and of the Council)

Pursuant to Article 3 of Regulation (EU) 2021/784 (the 'Regulation') the addressee of this removal order shall remove terrorist content or disable access to terrorist content in all Member States as soon as possible and in any event within one hour of receipt of the removal order.

Pursuant to Article 6 of the Regulation the addressee shall preserve content and related data, which has been removed or access to which as been disabled, for six months or longer upon request from the competent authorities or courts.

Pursuant to Article 15(2) of the Regulation, this removal order shall be sent in one of the languages designated by the addressee.

SECTION A:

Member State of the issuing competent authority:

.....

NB: details of the issuing competent authority to be provided in Sections E and F

Addressee and, where relevant, legal representative:

.....

Contact point:

.....

Member State where the hosting service provider has its main establishment or where its legal representative resides or is established:

.....

Time and date of issuing of the removal order:

.....

Reference number of the removal order:

.....

SECTION B: Terrorist content to be removed or access to which is to be disabled in all Member States as soon as possible and in any event within one hour of receipt of the removal order

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

.....

Reasons for considering the material to be terrorist content, in accordance with point (7) of Article 2 of the Regulation.

The material (please tick the relevant box(es)):

☐ incites others to commit terrorist offences, such as by glorifying terrorist acts, by advocating the commission of such offences (point (7)(a) of Article 2 of the Regulation)

☐ solicits others to commit or to contribute to the commission of terrorist offences (point (7)(b) of Article 2 of the Regulation)

☐ solicits others to participate in the activities of a terrorist group (point (7)(c) of Article 2 of the Regulation)

☐ provides instruction 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 terrorist offences (point (7)(d) of Article 2 of the Regulation)

☐ constitutes a threat to commit one of the terrorist offences (point (7)(e) of Article 2 of the Regulation)

Additional information for considering the material to be terrorist content:

.....

.....

.....

SECTION C: Information to the content provider

Please note that (please tick the box, if applicable):

☐ for reasons of public security, the addressee **must refrain from informing the content provider** of the removal of or disabling of access to the terrorist content

If the box is not applicable, please see Section G for details of possibilities to challenge the removal order in the Member State of the issuing competent authority under national law (a copy of the removal order must be sent to the content provider, if requested)

SECTION D: Information to the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established

Please tick the relevant box(es):

☐ The Member State where the hosting service provider has its main establishment or where its legal representative resides or is established is other than the Member State of the issuing competent authority

☐ A copy of the removal order is sent to the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established

SECTION E: Details of the issuing competent authority

Type (please tick the relevant box):

☐ judge, court or investigating judge

☐ law enforcement authority

☐ other competent authority → please complete also Section F

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

Name of the issuing competent authority:

.....

Name of its representative and post held (title and grade):

.....

File No:

.....

Address:

.....

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

.....

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

.....

Email address: .....

Date: .....

Official stamp (if available) and signature [1]:

.....

[1] A signature is not necessary if the removal order is sent through authenticated submission channels that can guarantee the authenticity of the removal order.

SECTION F: Contact details for follow-up

Contact details of the issuing competent authority for feedback on the time of removal or the disabling of access, or to provide further clarification:

.....

Contact details of the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established:

.....

SECTION G: Information about redress possibilities

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

Competent body or court before which the removal order can be challenged:

.....

Deadline for challenging the removal order (days/months starting from):

.....

Link to provisions in national legislation:

.....

ANNEX II

FEEDBACK FOLLOWING REMOVAL OF OR DISABLING OF ACCESS TO TERRORIST CONTENT

(Article 3(6) of Regulation (EU) 2021/784 of the European Parliament and of the Council)

SECTION A:

Addressee of the removal order:

.....

Competent authority that issued the removal order:

.....

File reference of the competent authority that issued the removal order:

.....

File reference of the addressee:

.....

Time and date of receipt of removal order:

.....

SECTION B: Measures taken in compliance with the removal order

(Please tick the relevant box):

☐ the terrorist content has been removed

☐ access to the terrorist content has been disabled in all Member States

Time and date of the measure taken:

.....

SECTION C: Details of the addressee

Name of the hosting service provider:

.....

OR

Name of the legal representative of the hosting service provider:

.....

Member State of main establishment of the hosting service provider:

.....

OR

Member State of residence or establishment of the legal representative of the hosting service provider:

.....

Name of the authorised person:

.....

Email address of the contact point:

.....

Date:

.....

ANNEX III

INFORMATION ABOUT THE IMPOSSIBILITY TO EXECUTE THE REMOVAL ORDER

(Article 3(7) and (8) of Regulation (EU) 2021/784 of the European Parliament and of the Council)

SECTION A:

Addressee of the removal order:

.....

Competent authority that issued the removal order:

.....

File reference of the competent authority that issued the removal order:

.....

File reference of the addressee:

.....

Time and date of receipt of removal order:

.....

SECTION B: Non-execution

(1) The removal order cannot be executed within the deadline for the following reasons (please tick the relevant box(es)):

☐ *force majeure* or *de facto* impossibility not attributable to the hosting service provider, including for objectively justifiable technical or operational reasons

☐ the removal order contains manifest errors

☐ the removal order does not contain sufficient information

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

.....

(3) If the removal order contains manifest errors and/or does not contain sufficient information, please specify the errors and the further information or clarification necessary:

.....

SECTION C: Details of the hosting service provider or its legal representative

Name of the hosting service provider:

.....

OR

Name of the legal representative of the hosting service provider:

.....

Name of the authorised person:

.....

Contact details (email address):

.....

Signature:

.....

Time and date:

.....