EDRi Amendments on the proposal for a Regulation to prevent the dissemination of terrorist content online

Contents

1. Problem Framing

Commission Proposal	**EDRi-Amendments**
Title	
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on preventing the dissemination of terrorist content online	REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on preventing the dissemination of ***illegal*** terrorist content online
Recitals	
(2) Hosting service providers active on the internet play an *essential* important role in the digital economy by connecting business and citizens and by facilitating public debate and the distribution and receipt of information, opinions and ideas, contributing significantly to innovation, economic growth and job creation in the Union. However, their services are in certain cases abused ***by third parties*** to carry out illegal activities online. Of particular concern is the misuse of hosting service providers by terrorist groups and their supporters to disseminate terrorist content online in order to spread their message, to ***radicalise and*** recruit and to facilitate and direct terrorist activity.	(2) Hosting service providers active on the internet play an *essential* role in the digital economy by connecting business and citizens and by facilitating public debate and the distribution and receipt of information, opinions and ideas, contributing significantly to innovation, economic growth and job creation in the Union. However, their services are in certain cases abused to carry out illegal activities online. Of particular concern is the misuse of hosting service providers by terrorist groups and their supporters to disseminate terrorist content online in order to spread their message, to recruit and to facilitate and direct terrorist activity.
(3) In ***light of*** their ***central*** role and the technological means and capabilities associated with the services they provide, online service providers ***have particular societal responsibilities*** to protect their services from misuse by terrorists and to help tackle terrorist content disseminated through their services, as part of a predictable and accountable framework that respects the rule of law and fundamental rights.	(3) In ***line with*** their role and the technological means and capabilities associated with the services they provide, online service providers ***could help competent authorities to*** protect their services from misuse by terrorists and to help tackle terrorist content disseminated through their services***, as long as this is*** *part of a predictable and accountable framework that respects the rule of law and fundamental rights****, including rules to assess the proportionality, efficiency and suitability of the measures chosen.***
Article 1 – paragraph 1	

1. This Regulation lays down ***uniform*** rules to ***prevent*** the misuse of hosting services for the dissemination of terrorist content online. It lays down in particular:	1. This Regulation lays down rules to ***tackle*** the misuse of hosting services for the dissemination of ***illegal*** terrorist content online. It lays down in particular:
2.This Regulation shall apply to hosting service providers ***offering*** services ***in*** the Union, irrespective of their place of main establishment.	2.This Regulation shall apply to hosting service providers ***targeting*** services ***in*** the Union, irrespective of their place of main establishment.
Article 1 – paragraph 1 a	
(a) rules on duties of care to be applied by hosting service providers in order to prevent the dissemination of terrorist content through their services and ensure, where necessary, its swift removal;	***deleted***
Article 1 – paragraph 1 b	
(b) a set of measures to be put in place by Member States to identify terrorist content, to enable its ***swift*** removal by hosting service providers and to facilitate cooperation with the competent authorities in other Member States, hosting service providers and where appropriate relevant Union bodies.	(b) a set of measures to be put in place by Member States to identify ***illegal*** terrorist content, to enable its removal by hosting service providers ***in accordance with Union law providing suitable safeguards for fundamental rights*** and to facilitate cooperation with the competent ***judicial or administrative*** authorities in other Member States, hosting service providers and where appropriate relevant Union bodies.

2. Scope and Definitions

2.1. Definition of a hosting service provider

Commission Proposal	EDRi-Amendments
Recitals	
(1) This Regulation ***aims at ensuring the smooth functioning of the digital single market in an open and democratic society, by tackling illegal content online and preventing the misuse of hosting services for terrorist purposes.*** The functioning of the digital single market should be improved by reinforcing legal certainty for hosting service providers, reinforcing users' trust in the online environment, and by strengthening safeguards to ~~the~~ freedom of expression and information.	(1) This Regulation ***contributes to the fight against terrorism by preventing the misuse of hosting service providers for spreading illegal terrorist content.*** The functioning of the digital single market should be improved by reinforcing legal certainty for hosting service providers, reinforcing users' trust in the online environment, and by strengthening safeguards to ***fundamental rights including*** freedom of expression and information***, the rights to privacy and to personal data protection.***
(7) This ***Regulation contributes*** to the protection of public security while establishing appropriate and robust safeguards to ensure protection of the fundamental rights at stake. This includes the rights to respect for private life and to the protection of personal data, the right to effective judicial protection, the right to freedom of expression, including the freedom to receive and impart information, the freedom to conduct a business, and the principle of non-discrimination. Competent authorities and hosting service providers should only adopt measures which are necessary, appropriate and proportionate within a democratic society, taking into account the particular importance accorded to the freedom of expression and information, which constitute***s*** one of the essential foundations of a pluralist, democratic society, and is one of the values on which the Union is founded. Measures ***constituting interference in the freedom of expression and information should be strictly targeted, in the sense that they must prevent the dissemination of terrorist content,*** but without thereby affecting the right to lawfully receive and impart information, taking into account the central role of hosting service providers in	(7) This ***Regulation's goal is to contribute*** to the protection of public security while establishing appropriate and robust safeguards to ensure protection of the ***rule of law and of*** fundamental rights at stake. This includes the rights to respect for private life and to the protection of personal data, the right to effective judicial protection, the right to freedom of expression, including the freedom to receive and impart information, the freedom to conduct a business, and the principle of non-discrimination. Competent authorities ***as defined in this Regulation*** and hosting service providers, ***in the pursuit of their legal obligations under this Regulation,*** 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***, the rights to privacy and to personal data protection*** which constitute one of the essential foundations of a pluralist, democratic society, and is one of the values on which the Union is founded. Measures ***taken to remove illegal terrorist content online should be necessary, appropriate and proportionate to help the fight against terrorism,***

facilitating public debate and the distribution and receipt of facts, opinions and ideas in accordance with the law.	***including investigation and prosecution of terrorist offences,*** but without thereby affecting the right to lawfully receive and impart information, taking into account the central role of hosting service providers in facilitating public debate and the distribution and receipt of facts, opinions and ideas in accordance with the law.
(10) In order to cover those online hosting services where terrorist content is disseminated, this Regulation should apply to information society services ***which store*** information provided by a recipient of the service at his or her request and in making the information stored available to ***third parties,***to the public ***irrespective of whether this activity is of a mere technical, automatic and passive nature***. By way of example such providers of information society services include social media platforms, video streaming services, video, image and audio sharing services~~,~~ ***file sharing and other cloud services*** to the extent they make the information available ***to third parties and websites where users can make comments or post reviews.*** The Regulation should also apply to hosting service providers established outside the Union but offering services within the Union, since a significant proportion of hosting service providers ~~exposed to~~ terrorist content on their services are established in third countries. This should ensure that all companies operating in the ***Digital Single Market*** comply with the same requirements, irrespective of their country of establishment. The determination as to whether a service provider offers services in the Union requires an assessment whether the service provider enables legal or natural persons in one or more Member States to use its services. However, the mere accessibility of a service provider's website or of an email address and of other contact details in one or more Member States taken in isolation should not be a sufficient condition for the application of this Regulation.	(10) In order to cover those online hosting services where terrorist content is disseminated, this Regulation should apply to information society services ***whose main business activity consists in the storage*** information provided by a recipient of the service at his or her request and in making the information stored available to the public. By way of example such providers of information society services include social media platforms, video streaming services, video, image and audio sharing services, to the extent they make the information available ***publicly***. The Regulation should also apply to hosting service providers established outside the Union but offering services within the Union, since a significant proportion of hosting service providers ***hosting illegal*** terrorist content on their services are established in third countries. This should ensure that all companies operating in the ***Union*** comply with the same requirements, irrespective of their country of establishment. The determination as to whether a service provider offers services in the Union requires an assessment whether the service provider enables legal or natural persons in one or more Member States to use its services. However, the mere accessibility of a service provider's website or of an email address and of other contact details in one or more Member States taken in isolation should not be a sufficient condition for the application of this Regulation.
Article 2 – paragraph 1	
For the purposes of this Regulation, the following definitions shall apply: (1) 'hosting service provider' means ***a provider of*** information society	For the purposes of this Regulation, the following definitions shall apply: (1)'hosting service provider' means ***any natural or legal person providing***

services consisting in the storage of information provided by and at the request of the content provider and in making the information stored available to ***third parties***;	information society services consisting in the storage of information provided by and at the request of the content provider and in making the information stored available to ***the public***;

2.2. Definition of illegal terrorist content

Commission Proposal	**EDRi-Amendments**
Recitals	
(9) In order to provide clarity about the actions that both hosting service providers and competent authorities should take to prevent the dissemination of terrorist content online, this Regulation should establish a definition of terrorist content ***for preventative purposes drawing*** on the definition of terrorist offences under Directive (EU) 2017/541 of the European Parliament and of the Council. Given the need to address ***the most harmful*** terrorist ***propaganda*** online, the definition should be rigorously consistent with existing instruments should capture material and information that incites, encourages or advocates the commission or contribution to terrorist offences, provides ***instructions*** for the commission of such offences or ***promotes the participation in activities of*** a terrorist group. Such information includes in particular text, images, sound recordings and videos. When assessing whether content constitutes illegal terrorist content within the meaning of this Regulation, competent authorities as well as hosting service providers must base their assessment on should take into account factors such as the notion of intention, the nature and wording of the statements, the context in which the statements were made and their demonstrable ***potential to lead to*** harmful consequences , thereby affecting the security and safety of persons. The fact that the material was produced by, is attributable to or disseminated on behalf of an EU-listed terrorist organisation or person constitutes an important factor in the assessment. Content disseminated for educational,	(9) In order to provide clarity about the actions that both hosting service providers and competent authorities should take to prevent the dissemination of terrorist content online, this Regulation should establish a definition of terrorist content ***based*** on the definition of terrorist offences under Directive (EU) 2017/541 of the European Parliament and of the Council. Given the need to address the ***illegal*** terrorist ***content*** online, the definition should be rigorously consistent with existing instruments should capture material and information that incites, encourages or advocates the commission or contribution to terrorist offences, provides ***training*** for the commission of such offences or ***recruits for*** a terrorist group. Such information includes in particular text, images, sound recordings and videos. When assessing whether content constitutes illegal terrorist content within the meaning of this Regulation, competent authorities as well as hosting service providers must base their assessment on should take into account factors such as the notion of intention, the nature and wording of the statements, the context in which the statements were made and their demonstrable ***risk of provoking actions with*** harmful consequences, thereby affecting the security and safety of persons. The fact that the material was produced by, is attributable to or disseminated on behalf of an EU-listed terrorist organisation or person constitutes an important factor in the assessment. Content disseminated for educational, parodic, journalistic or research purposes should be adequately protected,

parodic, journalistic or research purposes should be adequately protected, fall outside of the scope of this Regulation and, in particular, of the definition of illegal terrorist content and should be adequately protected. Furthermore, the expression of radical, polemic or controversial views in the public debate on sensitive political questions should not be considered terrorist content,	fall outside of the scope of this Regulation and, in particular, of the definition of illegal terrorist content and should be protected, ***in line with CJEU and ECtHR case law***. Furthermore, the expression of radical, polemic or controversial views in the public debate on sensitive political questions should not be considered terrorist content ***and equally falls outside of the scope of this Regulation and should be protected, in line with CJEU and ECtHR case law.***
Article 2 – paragraph 5	
(5) 'terrorist content' means one or more of the following information: ***(a)inciting or advocating, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed;*** ***(b) encouraging the contribution to terrorist offences;*** ***(c) promoting the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Article 2(3) of Directive (EU) 2017/541;*** ***(d) instructing on methods or techniques for the purpose of committing terrorist offences.***	(5) '***illegal*** terrorist content' means one or more of the following information: (***a) inciting unlawfully and intentionally the commission of terrorist offences within the meaning of Directive 2017/541 Article 3(1), where such conduct, whether or not expressly advocating the commission of terrorist offences, manifestly causes clear, substantial and imminent danger that one or more such offences be committed and is punishable as a criminal offence when committed unlawfully and intentionally*** ***(b) distributing or otherwise making available by other means online, a message to the public, with the clear intent to:*** ***- recruit for terrorism within the meaning of Directive2017/541 Article 6;*** ***- provide training for terrorism within the meaning of Directive 2017/541 Article 7*** ***- organise or otherwise facilitate travelling for the purpose of terrorism within the meaning of Directive 2017/541 Article 10.***
Article 2 – paragraph 6	

(6) ‘dissemination of terrorist content’ means making terrorist content available to ***third parties*** on the hosting service providers’ services;	(6) ‘dissemination of ***illegal*** terrorist content’ means making ***illegal*** terrorist content available to ***the public*** on the hosting service providers’ services;

3. Enforcement Measures

3.1. Legal Orders

Commission Proposal	**EDRi-Amendments**
Recitals	
(13) The procedure and obligations resulting from legal orders requesting hosting service providers to remove terrorist content or disable access to it, following ***an*** assessment by the competent authorities, should be harmonised. Member States should ***remain free*** *as to the choice of the* competent authorities ***allowing them to designate administrative, law enforcement or*** judicial authorities with that task. Given the speed at which terrorist content is disseminated across online services, this provision imposes obligations on hosting service providers to ensure that terrorist content identified in the removal order is removed or access to it is disabled within one hour from receiving the removal order. It is for the hosting service providers to decide whether to remove the content in question or disable access to the content for users in the Union.	(13) The procedure and obligations resulting from legal orders requesting hosting service providers to remove terrorist content or disable access to it, following ***a legal*** assessment by the competent authorities, should be harmonised. Member States should ***designate*** as to the choice of the competent authorities ***among their independent administrative and*** judicial authorities with that task. Given the speed at which terrorist content is disseminated across online services, this provision imposes obligations on hosting service providers to ensure that ***illegal*** terrorist content identified in the removal order is removed or access to it is disabled ***starting from*** one hour from receiving the removal order ***depending on the capacities of the company in question***. It is for the hosting service providers to decide whether to remove the content in question or disable access to the content for users in the Union ***based on the definition of illegal terrorist content, the implementation of effective redress mechanisms and generally taking as a basis of their decision any other applicable provisions from this Regulation***.
(14) The competent authority should transmit the removal order directly to the addressee and point of contact by ***any*** electronic means capable of	(14) The competent authority should transmit the removal order directly to the addressee and point of contact by ***identified secure*** electronic means

producing a written record under conditions that allow the service provider to establish authenticity, including the accuracy of the date and the time of sending and receipt of the order, such as by secured ***email and platforms or*** other secured channels, including those made available by the service provider, in line with the rules protecting personal data. This requirement may notably be met by the use of qualified electronic registered delivery services as provided for by Regulation (EU) 910/2014 of the European Parliament and of the Council 12 .	capable of producing a written record under conditions that allow the service provider to establish authenticity, including the accuracy of the date and the time of sending and receipt of the order, such as by secured channels, including those made available by the service provider, in line with the rules protecting personal data. This requirement may notably be met by the use of qualified electronic registered delivery services as provided for by Regulation (EU) 910/2014 of the European Parliament and of the Council 12.
(21) The obligation to preserve the content for proceedings of administrative or judicial review is necessary and justified in view of ensuring the effective measures of redress for the content provider whose content was removed or access to it disabled as well as for ensuring the reinstatement of that content as it was prior to its removal depending on the outcome of the review procedure. The obligation to preserve content for investigative and prosecutorial purposes is justified and necessary in view of the value this material could bring for the purpose of disrupting or preventing terrorist activity. Where companies remove material or disable access to it, in particular through their own ***proactive*** measures, and do not inform the ***relevant*** authority because they assess that it does not fall in the scope of Article 13(4) of this Regulation, law enforcement may be unaware of the existence of the content. Therefore, the preservation of content for purposes of prevention, detection, investigation and prosecution of terrorist offences is also justified. For these purposes, the required preservation of data is limited to data that is likely to have a link with terrorist offences, and can therefore contribute to prosecuting terrorist offences or to preventing serious risks to public security.	(21) The obligation to preserve the content for proceedings of ***competent independent*** administrative or judicial review is necessary and justified in view of ensuring the effective measures of redress for the content provider whose content was removed or access to it disabled as well as for ensuring the reinstatement of that content as it was prior to its removal depending on the outcome of the review procedure. The obligation to preserve content for investigative and prosecutorial purposes is justified and necessary in view of the value this material could bring for the purpose of disrupting or preventing terrorist activity. Where companies remove material or disable access to it, in particular through their own measures, and do not inform the ***competent independent administrative or judicial*** authority because they assess that it does not fall in the scope of Article 13(4) of this Regulation, law enforcement may be unaware of the existence of the content. Therefore, the preservation of content for purposes of prevention, detection, investigation and prosecution of terrorist offences is also justified. For these purposes, the required preservation of data is limited to data that is likely to have a link with terrorist offences, and can therefore contribute to prosecuting terrorist

	offences or to preventing serious risks to public security.
Article 4 – paragraph 2	
Hosting service providers shall remove terrorist content or disable access to it ***within one hour from receipt of the removal order.***	2. Hosting service providers shall remove ***in an expeditious manner illegal*** terrorist content or disable access to it.
Article 4 – paragraph 3	
3. Removal orders shall contain the following elements in accordance with the template set out in Annex I: (a) identification of the competent authority issuing the removal order and authentication of the removal order by the competent authority; (b) a statement of reasons explaining why the content is considered terrorist content, ***at least, by reference to the categories of terrorist content listed in Article 2(5);*** (c) a Uniform Resource Locator (URL) and, where necessary, additional information enabling the identification of the content referred; (d) a reference to this Regulation as the legal basis for the removal order; (e) date and time stamp of issuing; (f) information about redress available to the hosting service provider and to the content provider; (g) where ***relevant***, the decision not to disclose information about the removal of terrorist content or the disabling of access to it referred to in Article 11.	3. Removal orders shall contain the following elements in accordance with the template set out in Annex I: (a) identification of the competent authority issuing the removal order and authentication of the removal order by the competent authority; (b) a statement of reasons explaining why the content is considered ***illegal*** terrorist content; (c) a Uniform Resource Locator (URL) and, where necessary, additional information enabling the identification of the content referred; (d) a reference to this Regulation as the legal basis for the removal order; (e) date and time stamp of issuing; (f) information about redress available to the hosting service provider and to the content provider; (g) where ***necessary and appropriate***, the decision not to disclose information about the removal of terrorist content or the disabling of access to it referred to in Article 11. ***(h) deadlines for appeal for the hosting service provider and for the***

	content provider.
Art. 4 – paragraph 4	
4. ***Upon request by the*** hosting service provider or by the content provider, the competent authority shall provide a detailed statement of reasons, without prejudice to the obligation of the hosting service provider to comply with the removal order within the deadline set out in paragraph 2.	4. ***The*** hosting service provider or by the content provider, the competent authority shall provide a detailed statement of reasons, without prejudice to the obligation of the hosting service provider to comply with the removal order within the deadline set out in paragraph 2.
Article 4 – paragraph 7	
7. If the hosting service provider ***cannot*** comply with the removal order because of force majeure ***or*** of de facto impossibility not attributable to the hosting service provider, it shall inform, without undue delay, the competent authority, explaining the reasons, using the template set out in Annex III. The deadline set out in paragraph 2 shall apply as soon as the reasons invoked are no longer present.	7. If the hosting service provider ***refuses to*** comply with the removal order because of force majeure or of de facto impossibility not attributable to the hosting service provider***, or because of the impossibility to clearly determine the legality of the request or of violation of fundamental rights,*** it shall inform, without undue delay, the competent authority, explaining the reasons, using the template set out in Annex III. The deadline set out in paragraph 2 shall apply as soon as the reasons invoked are no longer present.
Article 4 – paragraph 8	
8. If the hosting service provider ***cannot*** comply with the removal order because the removal order contains manifest errors or does not contain sufficient information to execute the order, it shall inform the competent authority without undue delay, asking for the necessary clarification, using the template set out in Annex III. The deadline set out in paragraph 2 shall apply as soon as the clarification is provided.	8. If the hosting service provider ***refuses to*** comply with the removal order because the removal order contains manifest errors***,*** does not contain sufficient information to execute the order ***or because of the impossibility to clearly determine the legality of the request*** it shall inform the competent authority without undue delay, asking for the necessary clarification, using the template set out in Annex III. The deadline set out in paragraph 2 shall apply as soon as the clarification is

	provided.
Article 4 – paragraph 9	
9. ***The competent authority which issued the removal order shall inform the competent authority which oversees the implementation of proactive measures, referred to in Article 17(1)(c) when the removal order becomes final.*** A removal order becomes final where it has not been appealed within the deadline according to the applicable national law or where it has been confirmed following an appeal.	9. A removal order becomes final where it has not been appealed within the deadline according to the applicable national law or where it has been confirmed following an appeal.
Article 17 – paragraph 1	
1. Each Member State shall designate ***the authority*** or ***authorities*** competent to	1. Each Member State shall designate ***a judicial*** or ***an independent administrative authority*** competent to
Article 17 – paragraph 1 b	
(b) detect, identify and refer terrorist content to hosting service providers pursuant to Article 5;	***deleted***

3.2. Referrals

Commission Proposal	**EDRi-Amendments**
Recitals	
(15) ***Referrals by the competent authorities or Europol constitute an effective and swift means of making hosting service providers aware of***	***deleted***

specific content on their services. This mechanism of alerting hosting service providers to information that may be considered terrorist content, for the provider's voluntary consideration of the compatibility its own terms and conditions, should remain available in addition to removal orders. It is important that hosting service providers assess such referrals as a matter of priority and provide swift feedback about action taken. The ultimate decision about whether or not to remove the content because it is not compatible with their terms and conditions remains with the hosting service provider. In implementing this Regulation related to referrals, Europol's mandate as laid down in Regulation (EU) 2016/794[13] remains unaffected.	
(38) Penalties ***are*** necessary to ensure the effective implementation by hosting service providers of the obligations pursuant to this Regulation. Member States should adopt rules on penalties, including, where appropriate, fining guidelines. Particularly severe penalties shall be ascertained in the event that the hosting service provider systematically fails to remove terrorist content or disable access to it ***within one hour from receipt of a removal order***. Non-compliance in individual cases could be sanctioned while respecting the principles of ne bis in idem and of proportionality and ensuring that such sanctions take account of systematic failure. In order to ensure legal certainty, the regulation should set out to what extent the relevant obligations can be subject to penalties. ***Penalties for non-compliance with Article 6 should only be adopted in relation to obligations arising from a request to report pursuant to Article 6(2) or a decision imposing additional proactive measures pursuant to Article 6(4).*** When determining whether or not financial	(38) Penalties ***can be*** necessary to ensure the effective implementation by hosting service providers of the obligations pursuant to this Regulation. Member States should adopt rules on penalties, including, where appropriate, fining guidelines. Particularly severe penalties shall be ascertained in the event that the hosting service provider systematically fails to remove terrorist content or disable access to it ***within a reasonable amount of time, depending on the size and means of the hosting service provider***. Non-compliance in individual cases could be sanctioned while respecting the principles of ne bis in idem and of proportionality and ensuring that such sanctions take account of systematic failure. In order to ensure legal certainty, the regulation should set out to what extent the relevant obligations can be subject to penalties. When determining whether or not financial penalties should be imposed, due account should be taken of the financial resources of the provider. Member States shall ensure that penalties do not encourage the removal of content which is not

penalties should be imposed, due account should be taken of the financial resources of the provider. Member States shall ensure that penalties do not encourage the removal of content which is not terrorist content.	***illegal*** terrorist content.
Article 2 – paragraph 8	
8) 'referral' means a notice by a competent authority or, where applicable, a relevant Union body to a hosting service provider about information that may be considered terrorist content, for the provider's voluntary consideration of the compatibility with its own terms and conditions aimed to prevent dissemination of terrorism content;	***deleted***
Article 3	
Article 3 ***Duties of care*** ***1. Hosting service providers shall take appropriate, reasonable and proportionate actions in accordance with this Regulation, against the dissemination of terrorist content and to protect users from terrorist content. In doing so, they shall act in a diligent, proportionate and non-discriminatory manner, and with due regard to the fundamental rights of the users and take into account the fundamental importance of the freedom of expression and information in an open and democratic society.*** ***2. Hosting service providers shall include in their terms and conditions, and apply, provisions to prevent the dissemination of terrorist content.***	***deleted***

Article 5	
Article 5 ***Referrals*** ***1. The competent authority or the relevant Union body may send a referral to a hosting service provider.*** ***2. Hosting service providers shall put in place operational and technical measures facilitating the expeditious assessment of content that has been sent by competent authorities and, where applicable, relevant Union bodies for their voluntary consideration.*** ***3. The referral shall be addressed to the main establishment of the hosting service provider or to the legal representative designated by the service provider pursuant to Article 16 and transmitted to the point of contact referred to in Article 14(1). Such referrals shall be sent by electronic means.*** ***4. The referral shall contain sufficiently detailed information, including the reasons why the content is considered terrorist content, a URL and, where necessary, additional information enabling the identification of the terrorist content referred.*** ***5. The hosting service provider shall, as a matter of priority, assess the content identified in the referral against its own terms and conditions and decide whether to remove that content or to disable access to it.*** ***6. The hosting service provider shall expeditiously inform the competent authority or relevant Union body of the outcome of the assessment and the timing of any action taken as a result of the referral.*** ***7. Where the hosting service provider considers that the referral does***	***deleted***

not contain sufficient information to assess the referred content, it shall inform without delay the competent authorities or relevant Union body, setting out what further information or clarification is required.	

3.3. Additional Measures

Commission Proposal	**EDRi-Amendments**
Recitals	
(8) The right to an effective remedy is enshrined in Article 19 TEU and Article 47 of the Charter of Fundamental Rights of the European Union. Each natural or legal person has the right to an effective judicial remedy before the competent national court against any of the measures taken pursuant to this Regulation**,** which can adversely affect the rights of that person. The right includes, in particular the possibility for hosting service providers and content providers to effectively contest the removal orders before the court of the Member State whose authorities issued the removal order.	(8) The right to an effective remedy is enshrined in Article 19 TEU and Article 47 of the Charter of Fundamental Rights of the European Union. Each natural or legal person has the right to an effective judicial remedy before the competent national court against any of the measures taken pursuant to this Regulation which can adversely affect the rights of that person. The right includes, in particular, ***in the context of this Regulation***, the possibility for ***users to contest the removal of content resulting from measures taken by the hosting service provider as foreseen in this Regulation and informed of effective means of remedies, both internal and before the court of the Member State of residence. It also includes the ability for*** hosting service providers and content providers to effectively contest the removal orders before the court of the Member State whose authorities issued the removal order, ***the court of the Member State where the hosting service provider is established or represented, or the court of the Member State of residence for the content provider.***

(16) Given the ***scale and speed necessary*** for effectively identifying and removing terrorist content, ***proportionate proactive measures, including by using automated means in certain cases, are an essential element in tackling terrorist content online. With a view to reducing the accessibility of terrorist content on their services,*** hosting service providers should ***assess whether it is appropriate to take proactive measures depending on the risks and level of exposure to terrorist content as well as to*** the effects on the rights of third parties and the public interest of information. ***Consequently, hosting service providers should determine what appropriate, effective and proportionate proactive measure should be put in place. This requirement*** **should** not imply a general monitoring obligation. ***In the context of this assessment, the absence of removal orders and referrals addressed to a hosting provider, is an indication of a low level of exposure to terrorist content.***	(16) Given the ***potential impacts on fundamental rights and the complexity*** for effectively identifying and removing ***illegal*** terrorist content, ***additional*** measures ***could be taken by*** hosting service providers ***as long as they are appropriate and proportionate and necessary to achieve for the goals aimed by this Regulation***. ***These measures*** **cannot** imply a general monitoring obligation.
(17) When putting in place ***proactive*** measures, hosting service providers should ensure that users' ***right*** to freedom of expression and information - including to freely receive and impart information - **is** preserved. In addition to any requirement laid down in the law, including the legislation on protection of personal data, hosting service providers should act with due diligence and implement safeguards, including notably human oversight and verifications, ***where appropriate,*** to avoid any unintended and erroneous decision leading to removal of content that is not terrorist content. ***This is of particular relevance when hosting service providers use automated means to detect terrorist content. Any decision to use automated means, whether taken by the hosting service provider itself or pursuant to a request by the competent authority, should be assessed***	(17) When putting in place ***additional*** measures, hosting service providers should ensure that users' ***rights*** to freedom of expression and information**,** - including to freely receive and impart information – **and** ***to privacy and to the protection of personal data*** **are** preserved. In addition to any requirement laid down in the law, including the legislation on protection of personal data, hosting service providers should act with due diligence and implement safeguards, including notably human oversight and verifications, to avoid any unintended and erroneous decision leading to removal of content that is not ***illegal*** terrorist content.

with regard to the reliability of the underlying technology and the ensuing impact on fundamental rights.	
(19) ***Following the request, the competent authority should enter into a dialogue with the hosting service provider about the necessary proactive measures to be put in place. If necessary, the competent authority should impose the adoption of appropriate, effective and proportionate proactive measures where it considers that the measures taken are insufficient to meet the risks. A*** **decision to** ***impose such specific proactive*** measures should not, ***in principle,*** lead to the imposition of a general ***obligation to monitor***, as provided in Article 15(1) of Directive 2000/31/EC. ***Considering the particularly grave risks associated with the dissemination of terrorist content, the decisions adopted by the competent authorities on the basis of this Regulation could derogate from the approach established in Article 15(1) of Directive 2000/31/EC, as regards certain specific, targeted measures, the adoption of which is necessary for overriding public security reasons.*** Before adopting such decisions, the competent authority should strike a fair balance between the public interest objectives and the fundamental rights involved, in particular, the freedom of expression and information and the freedom to conduct a business, and provide appropriate justification.	(19) ***The*** measures ***taken by the hosting service provider*** should not lead to the imposition of a general ***monitoring***, as provided in Article 15(1) of Directive 2000/31/EC. Before adopting such decisions, the competent authority should strike a fair balance between the public interest objectives and the fundamental rights involved, in particular, the freedom of expression and information***, the rights to privacy and personal data protection,*** and the freedom to conduct a business, and provide appropriate justification ***explaining why the measures proposed are necessary to achieve the objectives of this Regulation and how they are appropriate and proportionate***.
(20) The obligation on hosting service providers to preserve removed content and related data, should be laid down for specific purposes and limited in time to what is necessary. ***There is need to extend the preservation requirement to related data to the extent that any such data***	(20) The obligation on hosting service providers to preserve removed content and related data, should be ***stricly necessary to achieve the aims of this Regulation*****,** laid down for specific purposes and limited in time to what is necessary ***and proportionate.***

would otherwise be lost as a consequence of the removal of the content in question. Related data can include data such as 'subscriber data', including in particular data pertaining to the identity of the content provider as well as 'access data', including for instance data about the date and time of use by the content provider, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the content provider.	
(25) Complaint procedures constitute a necessary safeguard against erroneous removal of content protected under the freedom of expression and information. Hosting service providers should therefore establish user-friendly complaint mechanisms and ensure that complaints are dealt with promptly and in full transparency towards the content provider. ***The requirement for the hosting service provider to reinstate the content where it has been removed in error, does not affect the possibility of hosting service providers to enforce their own terms and conditions on other grounds.***	(25) Complaint procedures constitute a necessary safeguard against erroneous removal of content protected under the freedom of expression and information. Hosting service providers should therefore establish user-friendly complaint mechanisms and ensure that complaints are dealt with promptly and in full transparency towards the content provider. ***Given the limitations of counter-notices as a safeguard for freedom of expression, hosting services providers shall also provide the user with detailed information on access to effective remedies, including judicial redress in front of an independent court.***
(26) Effective legal protection according to Article 19 TEU and Article 47 of the Charter of Fundamental Rights of the European Union requires that persons are able to ascertain the reasons upon which the content uploaded by them has been removed or access to it disabled. For that purpose, the hosting service provider should make available to the content provider meaningful information enabling the content provider to contest the decision***. However, this does not necessarily require*** a notification ***to the content provider***. ***Depending on the circumstances, hosting*** service	(26) Effective legal protection according to Article 19 TEU and Article 47 of the Charter of Fundamental Rights of the European Union requires that persons are able to ascertain the reasons upon which the content uploaded by them has been removed or access to it disabled. For that purpose, the hosting service provider should make available to the content provider ***detailed, complete and*** meaningful information enabling the content provider to contest the decision***, including*** a notification. ***Hosting*** service providers may replace content which is considered terrorist content, with a

providers may replace content which is considered terrorist content, with a message that it has been removed or disabled *in accordance with this Regulation*. Further information about the reasons as well as possibilities for the content provider to contest the decision should be given ***upon request***. Where competent authorities decide that for reasons of public security including in the context of an investigation, it is considered ***inappropriate or counter-productive*** to directly notify the content provider of the removal or disabling of content**, they should inform the hosting service provider**.	message that it has been removed or disabled ***following the issuing of a removal order and in accordance with this Regulation***. Further information about the reasons as well as possibilities for the content provider to contest the decision should be given ***unless the competent authority reasonably asks otherwise***. Where competent authorities decide that for reasons of public security including in the context of an investigation, it is considered ***inappropriate or counter-productive*** to **not** directly notify the content provider of the removal or disabling of content ***exclusively during the necessary period of time requested by the competent authorities to ensure the gathering of evidence or any other measure necessary to ensure the investigation of potential terrorist activities.*** .
Article 6 – title	
Article 6 ***Proactive*** *measures*	*Article 6* ***Additional*** *measures*
Article 6 – paragraph 1	
1. Hosting service providers ***shall***, ***where appropriate,*** take ***proactive*** measures to protect their services against the dissemination of terrorist content. The measures shall be effective and proportionate**, *taking into account*** the risk and level of exposure to terrorist content, the fundamental rights of the users, and the fundamental importance of the freedom of expression and information in an open and democratic society.	1. Hosting service providers ***may***, *where a significant number of removal orders have been directed at their service***,** take ***additional*** measures to protect their services against the dissemination of terrorist content. The measures shall be effective, ***targeted*** and proportionate **to** the risk and level of exposure to terrorist content, ***and duly respecting*** the fundamental rights of the users, and the fundamental importance of the freedom of expression and information ***and rights to privacy and personal data protection*** in an open and democratic society.

Article 6 – paragraph 2	
2. Where it has been informed according to Article 4(9), the competent authority referred to in Article 17(1)(c) shall request the hosting service provider to submit a report***, within three months after receipt of the request and thereafter at least*** on an annual basis, on the specific ***proactive*** measures it has taken***, including by using automated tools, with a view to:*** ***(a) preventing the re-upload of content which has previously been removed or to which access has been disabled because it is considered to be terrorist content;*** ***(b) detecting, identifying and expeditiously removing or disabling access to terrorist content.*** ***Such a request shall be sent to the main establishment of the hosting service provider or to the legal representative designated by the service provider.*** The reports shall include all relevant information allowing the competent authority referred to in Article 17(1)(c) to assess whether the ***proactive*** measures ***are effective*** and proportionate, including ***to evaluate*** the functioning of any automated tools used as well as the human oversight and verification mechanisms employed.	***2. T***he hosting service provider ***shall*** submit a report on an annual basis, on the specific measures it has taken ***to the competent authority.*** The reports shall include all relevant information allowing the competent authority referred to in Article 17(1)(c) to assess whether the ***additional*** measures ***effectively contribute to tackling illegal terrorist content online and are necessary and proportionate,*** including ***an annual report that includes an evaluation of the nature and functioning measures* i*t has taken, how many removals have led to criminal investigations, and how many of those have ended in criminal convictions, as well as information on the the number of reinstated content and*** the human oversight***, review mechanisms accessed by individuals affected by removals and the outcome of the process*** and ***any*** verification mechanisms employed ***to assess the illegality of the terrorist content removed or whose access has been disabled***.
Article 6 – paragraph 3	
3. Where the competent authority referred to in Article 17(1)(c) considers that the ***proactive*** measures taken and reported under paragraph 2 ***are***	3. Where the competent authority referred to in Article 17(1)(c) considers that the measures taken and reported under paragraph 2 ***do not respect***

insufficient in mitigating and managing the risk and level of exposure, it may request the hosting service provider to ***take specific*** additional ***proactive*** measures. For that purpose, the hosting service provider shall cooperate with the competent authority referred to in Article 17(1)(c) with a view to identifying the specific measures that the hosting service provider shall put in place, ***establishing*** key objectives and benchmarks as well as timelines for their implementation.	***the principles of necessity, appropriateness and proportionality, or that the risks and level of exposures remain unchanged*** it may request the hosting service provider to ***re-evaluate the*** measures ***needed*** . For that purpose, the hosting service provider shall cooperate with the competent authority referred to in Article 17(1)(c) with a view to identifying the specific measures that the hosting service provider ***shall consider to*** put in place, ***including suggestions for*** key objectives and benchmarks as well as timelines for their implementation.
Article 6 – paragraph 4	
4. Where no agreement can be reached within the three months from the request pursuant to paragraph 3, the competent authority referred to in Article 17(1)(c) may issue a decision imposing specific additional necessary and proportionate ***proactive*** measures. The decision shall take into account, in particular, the economic capacity of the hosting service provider and the effect of such measures on the fundamental rights of the users and the fundamental importance of the freedom of expression and information. Such a decision shall be sent to the main establishment of the hosting service provider or to the legal representative designated by the service provider. The hosting service provider shall regularly report on the implementation of such measures as specified by the competent authority referred to in Article 17(1)(c).	4. Where no agreement can be reached within the three months from the request pursuant to paragraph 3, the competent authority referred to in Article 17(1)(c) may issue a decision imposing specific additional necessary and proportionate measures ***that may not lead to impose general obligations to monitor***. The decision shall take into account, in particular, the economic capacity of the hosting service provider and the effect of such measures on the fundamental rights of the users and the fundamental importance of the freedom of expression and information***, as well as rights to privacy and personal data protection***. Such a decision shall be sent to the main establishment of the hosting service provider or to the legal representative designated by the service provider. The hosting service provider shall regularly report on the implementation of such measures as specified by the competent authority referred to in Article 17(1)(c).
Article 9, paragraph 1	
1. Where hosting service providers use ***automated*** tools pursuant to this Regulation in respect of content that they store, they shall provide	1. Where hosting service providers use tools pursuant to this Regulation in respect of content that they store, they shall provide effective

effective and ***appropriate*** safeguards to ensure that decisions taken concerning that content, in particular decisions to remove or disable content considered to be terrorist content, are accurate and well-founded.	safeguards to ensure that decisions taken concerning that content, in particular decisions to remove or disable content considered to be ***illegal*** terrorist content, are accurate and well-founded.
Article 9, paragraph 2	
2. Safeguards shall consist, in particular, of human oversight and verifications ***where appropriate and,*** in any event**,** where a detailed assessment of the relevant context is required in order to determine whether or not the content is to be considered terrorist content.	2. Safeguards shall consist, in particular, of human oversight and verifications ***of the illegality of the content as well as the balance of the decision to remove or deny access to content with the respect for fundamental rights and the rule of law. Human oversight shall be required*** in any event where a detailed assessment of the relevant context is required in order to determine whether or not the content is to be considered ***illegal*** terrorist content.
Article 10 – paragraph 1	
1. Hosting service providers shall establish effective and accessible mechanisms allowing content providers whose content has been removed or access to it disabled as a result of **a *referral*** pursuant to Article ***5*** or of ***proactive*** measures pursuant to Article 6, to submit a complaint against the action of the hosting service provider requesting reinstatement of the content.	1. Hosting service providers shall establish effective and accessible mechanisms allowing content providers whose content has been removed or access to it disabled as a result of ***additional*** measures pursuant to Article 6, to submit a complaint against the action of the hosting service provider requesting reinstatement of the content.
Article 10 – paragraph 2	
2. Hosting service providers shall promptly examine every complaint that they receive and reinstate the content without undue delay where the	2. Hosting service providers shall promptly examine every complaint that they receive and reinstate the content without undue delay where the

removal or disabling of access ***was unjustified***. ***They*** shall inform the complainant about the outcome of the examination.	removal or disabling of access ***is found not to be illegal terrorist content under Article 2 (5) of this Regulation***. ***The hosting service providers*** shall inform the complainant ***within two weeks from the receipt of the complaint*** about the outcome of the examination. ***A reinstatement of content shall not preclude further judicial measures against the decision of the hosting service provider or of the competent competent authority.***
Article 10 – paragraph 3 (new)	
	3. Notwithstanding the provisions of Art. 10 (1) and (2), the complaint mechanism of the hosting service providers shall be complementary to the applicable laws and procedures of the Member State in regard to the right to judicial review.
Article 11 – paragraph 2	
2. ***Upon request of the content provider, t***he hosting service provider shall inform the content provider ***about the reasons for the removal or disabling of access and possibilities to contest the decision.***	2. ***The*** hosting service provider shall inform the content provider
Article 11 – paragraph 2 a (new)	
	(a) about the reasons for the removal or disabling of access, including information on the legal basis for the removal or disabling of access
Article 11 – paragraph 2 b (new)	
	(b) about the possibilities to contest the decision, including information on the relevant entities involved in the decision and the deadlines for

	launching a complaint
Article 11 – paragraph 2 c (new)	
	(c) the legal basis within this Regulation upon which the removal was taken;
Article 13 – paragraph 1	
1. Competent authorities in Member States shall inform***,*** *coordinate* and cooperate with each other and, where appropriate, with relevant Union bodies such as Europol with regard to removal orders ***and referrals*** to avoid duplication, enhance coordination and avoid interference with investigations in different Member States.	1. Competent authorities in Member States shall inform, coordinate and cooperate with each other and, where appropriate, with relevant Union bodies such as Europol with regard to removal orders to avoid duplication, enhance coordination and avoid interference with investigations in different Member States.
Article 13 – paragraph 2	
2. Competent authorities in Member States shall inform, coordinate and cooperate with the competent authority referred to in Article 17(1)***(c) and (d)*** with regard to measures taken pursuant to Article 6 and enforcement actions pursuant to Article 18. Member States shall make sure that the competent authority referred to in Article 17(1)***(c) and*** *(d)* is in possession of all the relevant information. For that purpose, Member States shall provide for the appropriate communication channels or mechanisms to ensure that the relevant information is shared in a timely manner.	2. Competent authorities in Member States shall inform, coordinate and cooperate with the competent authority referred to in Article 17(1) with regard to measures taken pursuant to Article 6 and enforcement actions pursuant to Article 18. Member States shall make sure that the competent authority referred to in Article 17(1) ***(d)*** is in possession of all the relevant information. For that purpose, Member States shall provide for the appropriate communication channels or mechanisms to ensure that the relevant information is shared in a timely manner.
Article 13 – paragraph 3	

3. Member States and hosting service providers may choose to make use of dedicated tools, including, where appropriate, those established by relevant Union bodies such as Europol, to facilitate ***in particular:*** ***(a) the processing and feedback relating to removal orders pursuant to Article 4;*** ***(b)the processing and feedback relating to referrals pursuant to Article 5;*** ***(c)co-operation with a view to identify and implement proactive measures pursuant to Article 6.***	3. Member States and hosting service providers may choose to make use of dedicated tools, including, where appropriate, those established by relevant Union bodies such as Europol, to facilitate ***the processing and feedback relating to removal orders pursuant to Article 4;***

4. Transparency, accountability and efficiency monitoring

Commission Proposal	EDRi amendments
Recitals	
(18) In order to ensure that hosting service providers exposed to terrorist content take appropriate measures to ***prevent the misuse of their services,*** the competent authorities should request hosting service providers having received a removal order, which has become final, to report on **the** ***proactive*** measures taken. ***These could consist of measures to prevent the re-upload of terrorist content, removed or access to it disabled as a result of a removal order or referrals they received, checking against publicly or privately-held tools containing known terrorist content. They may also employ the use of reliable technical tools to identify new terrorist content, either using those available on the market or those developed by the hosting service provider.*** The service provider should report on the specific ***proactive*** measures in place in order to allow the competent authority to judge whether the measures are effective and proportionate and whether, if automated means are used, the hosting service provider has the necessary abilities for human oversight and verification. In assessing the effectiveness and proportionality of the measures, competent authorities should take into account relevant parameters including the number of removal orders ***and referrals*** issued to the provider, their economic capacity ***and*** the impact of its service in disseminating terrorist content (for example, taking into account the number of users in the Union).	(18) In order to ensure that hosting service providers exposed to ***illegal*** terrorist content take appropriate measures to ***tackle illegal terrorist content online,*** the competent authorities should request hosting service providers having received a removal order, which has become final, to report on any ***additional*** measures taken. The service provider should report on the specific ***additional*** measures in place in order to allow the competent authority to judge whether the measures are effective and proportionate and whether, if automated means are used, the hosting service provider has the necessary abilities for human oversight and verification. In assessing the effectiveness***, necessity*** and proportionality of the measures, competent authorities should take into account relevant parameters including the number of removal orders issued to the provider, their economic capacity***,*** the impact of its service in disseminating ***illegal*** terrorist content (for example, taking into account the number of users in the Union)***, the safeguards put in place to protect fundamental rights (namely the right to freedom of expression and information) and the incidences and restrictions on legal content.***
(24) Transparency of hosting service providers' policies in relation to	(24) Transparency of hosting service providers' policies in relation to

terrorist content is essential to enhance ***their*** accountability towards ***their*** users and to reinforce trust of citizens in the ***Digital Single Market***. Hosting service providers should publish annual transparency reports containing meaningful information about action taken in relation to the detection, identification and removal of terrorist content.	***illegal*** terrorist content is essential to enhance accountability towards users and to reinforce trust of citizens in ***hosting service providers' and competent authorities' in*** the ***Union***. Hosting service providers should publish annual transparency reports containing ***detailed and*** meaningful information about action taken in relation to the detection, identification and removal of ***illegal*** terrorist content ***and the potential legal content restrictions. Likewise, competent authorities should publish annual transparency reports containing detailed and meaningful information about the number of legal orders issued, the number of removals, the number of identified and detected illegal terrorist contents leading to investigation and prosecution of terrorist offences and the number of restrictions on legal content.***
Article 8 – paragraph 1	
1. Hosting service providers shall set out in their terms and conditions their policy to ***prevent*** the dissemination of terrorist content, includi***ng, where appropriate, a meaningful explanation of the functioning of proactive measures including the use of automated tools.***	1. Hosting service providers shall set out in their terms and conditions their policy to ***collaborate with the competent judicial or independent administrative authorities against*** the dissemination of ***illegal*** terrorist content, including a detailed ***and meaningful explanation of the functioning of additional measures. Where automated tools are used, such explanation must include a detailed and meaningful explanation of their functioning.***
Article 8 – paragraph 2	
2.Hosting service providers shall publish annual transparency reports on action taken against the dissemination of terrorist content.	2.Hosting service providers ***and the authorities competent to issue removal orders*** shall publish annual transparency reports on action taken

	against the dissemination of ***illegal*** terrorist content.
Article 8 – paragraph 3	
3.Transparency reports shall include at least the following information:	3. Transparency reports ***of hosting service providers*** shall include at least the following information:
Article 8 – paragraph 3 a	
(a) information about the hosting service provider's measures in relation to the ***detection, identification and*** removal of terrorist content;	(a) information about the hosting service provider's measures in relation to the removal of ***illegal*** terrorist content;
Article 8 – paragraph 3 b	
(b) information about the hosting service provider's measures to prevent the re-upload of content which has previously been removed or to which access has been disabled because it ***is considered*** to be terrorist content;	***Deleted***
Article 8 – paragraph 3 c	
(c) number of pieces of terrorist content removed or to which access has been disabled, following removal orders, ***referrals***, or ***proactive*** measures, respectively;	(c) number of pieces of ***illegal*** terrorist content removed or to which access has been disabled, following removal orders, or ***any additional*** measures, respectively;
Article 8 – paragraph 3 d	
(d) ***overview*** and outcome of complaint procedures.	(d) ***number of complaint procedures launched, a detailed overview on***

	the reasons for which complaint procedures were launched and ***the*** outcome of ***these*** complaint procedures***, including the final number of cases in which legal content was wrongly identified as illegal terrorist content ('false positives')***.
Article 8 – paragraph 4 (new)	
	4. Transparency reports of the competent authorities shall include at least the information transmitted to the Commission pursuant to Article 21 (1) of this Regulation.
Article 21 – paragraph 1	
1. Member States shall collect from their competent authorities and the hosting service providers under their jurisdiction ***and send to the Commission every year by [31 March]*** information about the actions they have taken in accordance with this Regulation. That information shall include:	1. Member States shall collect from their competent authorities and the hosting service providers under their jurisdiction information about the actions they have taken in accordance with this Regulation. ***The information shall be sent to the Commission every year by [31 March] and shall be published in the competent authorities' transparency reports pursuant to Article 8 (4) of this Regulation no later than two weeks after being sent to the Commission.*** The information shall include:
Article 21 – paragraph 1 a	
(a) information about the number of removal orders ***and referrals*** issued, the number of pieces of terrorist content which has been removed or access to it disabled, including the corresponding timeframe***s*** pursuant to Article***s*** 4 ***and 5***;	(a) information about the number of removal orders issued, the number of pieces of ***illegal*** terrorist content which has been removed or access to it disabled, including the corresponding timeframe pursuant to Article 4;
Article 21 – paragraph 1 b	
(b) information about the specific ***proactive*** measures taken pursuant to	(b)information about the specific ***additional*** measures taken pursuant to

Article 6, including the amount of terrorist content which has been removed or access to it disabled and the corresponding timeframes;	Article 6, including the amount of ***illegal*** terrorist content which has been removed or access to it disabled and the corresponding timeframes;
Article 21 – paragraph 1 b a (new)	
	(ba) information about the number of access requests issued by national competent authorities regarding content retained by the hosting service providers
Article 21 – paragraph1 b b (new)	
	(bb) information about the number of investigations and prosecutions initiated following the accessing of content retained by the hosting service providers
Article 21 – paragraph 2	
2. By [one year from the date of application of this Regulation] at the latest, the Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Regulation. The monitoring programme shall set out the indicators and the means by which and the intervals at which the data and other necessary evidence is to be collected. It shall specify the actions to be taken by the Commission and by the Member States in collecting and analysing the data and other evidence to monitor the progress and evaluate this Regulation pursuant to Article 23.	2. By [one year from the date of application of this Regulation] at the latest, the Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Regulation***, including an assessment of the impact on citizens' fundamental rights and freedoms and the Rule of Law in the Member States***. The monitoring programme shall set out the ***key performance*** indicators and the means by which and the intervals at which the data and other necessary evidence is to be collected. It shall specify the actions to be taken by the Commission and by the Member States in collecting and analysing the data and other evidence to monitor the progress and evaluate this Regulation pursuant to Article 23.
Article 23	
No sooner than [three years from the date of application of this	***[T***hree years from the date of application of this Regulation], the

Regulation], the Commission shall carry out an evaluation of this Regulation and submit a report to the European Parliament and to the Council on the application of this Regulation including the functioning of the effectiveness of the safeguard mechanisms. Where appropriate, the report shall be accompanied by legislative proposals. Member States shall provide the Commission with the information necessary for the preparation of the report.	Commission shall carry out an evaluation of this Regulation and submit a report to the European Parliament and to the Council on the application of this Regulation including the functioning of the effectiveness of the safeguard mechanisms. ***The report shall also cover the impact of this Regulation on fundamental rights and freedoms and on the rule of law situation in Member States.*** Where appropriate, the report shall be accompanied by legislative proposals. Member States***, experts and other stakeholders including from the human and digital rights field*** shall provide the Commission with the information necessary for the preparation of the report.