European Parliament

*25.02.2019*

**TKV/MB/cb**

# Final Compromise Amendments

on the Draft Opinion

**on preventing the dissemination of terrorist content online**

**2018/0331(COD)**

Rapporteur: Julia Reda

# Compromise amendments on IMCO draft Opinion on the proposal for a regulation on preventing the dissemination of terrorist content online

| ARTICLES | |
|---|---|
| CA 1 | Art. 1 |
| CA 2 | 2 (points 1, 4, 5 and 9a (new) only) |
| CA 3 | 3 |
| CA 4 | 4 |
| CA 5A | 4a (new) |
| CA 5B | 4a (new) |
| CA 6 | 5 |
| CA 7 | 6 |
| CA 8 | 7 |
| CA 9 | 8 |
| CA 10 | 8a (new) |
| CA 11 | 9 |
| CA 12 | 10 |
| CA 13 | 11 |
| CA 14 | 17 |
| CA 15 | 18 |
| CA 16 | Annex I (para 1, Section B, Section G only) |
| **RECITALS** | |
| CA A | Recital 1, 1a (new), 3, 4, 5, 6, 7, 7a (new), 7b (new), 8 |
| CA B | 9, 10 |
| CA C | 12 |
| CA D | 13, 13a (new) |
| CA E | 15 |
| CA F | 16, 17, 18, 19, 19a (new) |
| CA G | 24, 24a (new), 25, 26, |
| CA H | 37 |
| CA I | 38 |

**CA 1 covering Article 1**

**Replacing all relevant amendments, including: Rapp 35, Rapp 36, Rapp 37, Rapp 38, Rapp 39, Rapp 67, EPP 184, ECR 185, S&D 189, EPP 196, S&D 195, ECR 197, ALDE 194, Rapp 198, EPP 241**

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

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

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

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

***2a. The application of this Regulation shall be subject to Union law regarding fundamental rights, freedoms and values as enshrined in particular in Articles 2 and 6 of the Treaty on the European Union and shall not have the effect of modifying the obligations resulting therefrom. Member States may establish conditions required by, and in accordance with fundamental principles relating to freedom of the press and freedom and pluralism of the media.***

***2b. This Regulation is without prejudice to Directive 2000/31/EC.***

**CA 2 covering Article 2, points 1, 4, 5 and 9a (new)**

**Replacing all relevant amendments, including: Rapp 40-45, Rapp 48, EPP 200, ECR 203, S&D 192, S&D 208, ALDE 209, ALDE 210, ECR 143, 239 EPP**

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

(1) 'hosting service provider' means a provider of information society services ~~consisting~~ ***whose business activity consists*** in the storage ***and processing*** of information provided by and at the request of the content provider and in ~~making~~ ***disseminating*** the information stored ***to the public, and for which it is possible to identify and remove specific content.***

***In particular, for the purpose of this Regulation, providers of services at other layers of the Internet infrastructure than the application layer, and cloud IT infrastructure service providers shall not be considered as hosting service providers***;

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

(5) 'terrorist content' means ***information or material that constitutes*** one or more of the following ~~information~~ ***offences committed intentionally as defined in Articles 3 to 7 in Directive 2017/541, in particular by***:

(a) inciting ~~or advocating, including~~ ***the commission of one of the offences listed in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, where such conduct, directly or indirectly, such as*** ~~by glorifying,~~ 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) ***soliciting another person to commit*** or contribute to ***the commission of one of the offences listed in points (a) to (i) of Article 3(1), or in Article 4 of Directive (EU) 2017/541;***

(c) ***participating in*** the activities of a terrorist group***, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the*** terrorist group***,*** within the meaning of Article ***4*** of Directive (EU) 2017/541;

(d) ~~instructing on~~ ***providing 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 ***listed in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, knowing that the skills provided are intended to be used for this purpose, is punishable as a criminal offence when committed intentionally***.

***(9a) 'competent authority' means a single designated national judicial authority in the Member State, or an administrative authority.***

**CA 3 covering Article 3**

**Replacing all relevant amendments, including: Rapp 49, S&D 240, EPP 241, ECR 242**

1. Hosting service providers ***that are exposed to terrorist content*** 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 ***in all circumstances*** to the fundamental rights of the users and take into account the fundamental importance of the freedom of expression and information in an open and democratic society. ***Those actions shall not amount to a general obligation on hosting service providers to monitor the information, which they store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.***

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

**CA 4 covering Article 4**

**Replacing all relevant amendments, including: Rapp 51, Rapp 53, Rapp 54, Rapp 56, Rapp 59, Rapp 246, S&D 247, S&D 248 GUE 250, EPP 255, EPP 258, S&D 257, EPP 260, GUE 262, EPP 225, S&D 257 EPP 263, EPP 264, ECR 267, ECR 268, EPP 269, S&D 274, EPP 276, S&D 278, S&D 254**

*Article 4*

1. The competent authority shall have the power to issue a ~~decision~~ ***removal order*** requiring the hosting service provider to remove terrorist content or disable access to it ***and shall immediately inform the competent authorities of any other Member States whose interests it considers may be affected by the issuing of that removal order***.

***1a. Member States shall ensure that removal orders issued by an administrative authority are subject to a review by an independent judicial authority to assess the conformity with the definition of terrorist content pursuant to Article 2(5) and to revoke the removal order where appropriate.***

2. Hosting service providers shall remove terrorist content or disable access to it ~~within one hour from receipt of the removal order~~ ***expeditiously. The competent authority shall set a deadline for compliance with the removal order that shall be no shorter than 8 hours. When setting the deadline, the competent authority shall take due account of the size and resources of the hosting service provider, in particular that SMEs may require a longer time limit to comply with the removal order. In any event, the deadline shall be no sooner than the end of the next working day for***

***hosting service providers that have not previously been subject to a removal order and are microenterprises as defined in the Commission Recommendation 2003/361/EC, including sole traders.***

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 ***detailed*** statement of reasons explaining why the content is considered terrorist content; ~~at least~~, by ***specific*** reference to the categories of terrorist content listed in Article 2(5) ***and substantiating the elements of unlawfulness and intentionality and the relevant national law***;

   (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 and the time limit to comply with the removal order in accordance with paragraph 2;

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

   (g) where ~~relevant~~ ***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.

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

5. The competent authority shall address removal orders to the main establishment of the hosting service provider or to the legal representative designated by the hosting service provider pursuant to Article 16 and transmit it to the point of contact referred to in Article 14(1). Such orders shall be sent by electronic means capable of producing a written record under conditions allowing to establish the authentication of the sender, including the accuracy of the date and the time of sending and receipt of the order.

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

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

8. If the hosting service provider cannot comply with the removal order ***in instances when*** the removal order contains manifest errors or does not contain sufficient information to execute the order, it shall inform the competent authority ***immediately***, asking for the necessary clarification, using the template set out in Annex III. The ***hosting service provider*** shall ***remove the terrorist content or disable access to it expeditiously*** as soon as the clarification ***to the removal order*** is provided.

9. The competent authority which issued the removal order shall inform the competent authority which oversees the implementation of ~~proactive~~ ***specific*** 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 ***and redress has not been sought*** within the deadline according to the applicable national law or where it has been confirmed following an appeal.

**CA 5A covering Article 4a (new)**

**Replacing all relevant amendments, including: S&D 254, Rapp 279**

***Article 4a***
***Cross-border cooperation related to removal orders***

***1. Where a competent authority of a Member State other than the one in which the main establishment of the hosting service provider or its designated representative is located considers that terrorist content should be removed, it may ~~make the~~ request the competent authority of the Member State in which the main establishment of the hosting service provider or its designated representative is located to issue a removal order.***

***2. The competent authority of the Member State in which the main establishment of the hosting service provider or its designated representative is located may issue the removal order requested in accordance with paragraph 1 to the hosting service provider in accordance with Article 4 within two working days.***

***3. In cases where the competent authority of the Member State in which the main establishment of the hosting service provider or its designated representative is located does not issue the removal order, for example because it does not fulfil the conditions of Article 4(3) or because the competent authority has reasonable grounds to believe that the removal order may impact fundamental interests of that Member State or may affect fundamental rights of the individual, it shall inform the requesting competent authority accordingly.***

4. ***The requesting competent authority may turn to Europol in order to settle the dispute, adapt its request for issuance of a removal order, taking those circumstances into account, or it may withdraw it.***

**CA 5B covering Article 4a (new)**

**Replacing all relevant amendments, including: S&D 247, S&D 248, EPP 251, S&D 254**

*Article 4a*
*Cross-border cooperation related to removal orders*

1. ***The competent authority issuing the removal order to the hosting service provider shall submit immediately a copy of that removal order to the competent authority referred to in Article 17(1)(a) of the Member State in which the main establishment of the hosting service provider or its designated representative is located.***

2. ***In cases where the competent authority of the Member State in which the main establishment of the hosting service provider, its designated representative or the content provider is located has reasonable grounds to believe that the removal order may affect fundamental rights of the individual, it shall inform the requesting competent authority.***
3. ***The requesting competent authority shall take those circumstances into account and shall, where necessary, withdraw or adapt the removal request.***

**CA 6 covering Article 5**

**Replacing all relevant amendments, including: Rapp 60, ALDE 281, EPP 283, S&D 282, ALDE 286**

*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. ***The referral shall also be sent to the competent authority of the Member State in which the main establishment of the hosting service provider or its designated representative is located.***

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

5. The hosting service provider ***may*** ~~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 ***until the decision by the competent authority pursuant to paragraph 6a is made final***.

6. The hosting service provider shall ~~expeditiously~~ inform the competent authority or relevant Union body of ~~the outcome of the assessment~~ any action taken as a result of the referral, ***including when no action has been taken***.

***6a. The competent authority of the Member State in which the main establishment of the hosting service provider or its designated representative is located shall without undue delay assess whether the content that is subject to the referral constitutes terrorist content within the meaning of this Regulation. Following the assessment, the competent authority shall without undue delay either inform the hosting service provider that the content was deemed not to be terrorist content, or issue a removal order pursuant to Article 4.***

***6b. Hosting services providers shall not be held liable solely for complying with the provisions of this Article.***

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

**CA 7 covering Article 6**

**Replacing all relevant amendments, including: Rapp 19, Rapp 61, ALDE 288, GUE 289, ECR 290, S&D 291, ALDE 292, EPP 294, EPP 296, ALDE 297, EPP 299, EPP 303, ALDE 304, EPP 307, ALDE 308, EPP 309, EPP 315**

Article 6

~~Proactive~~ ***Specific*** measures

1. Hosting service providers shall**,** where appropriate ***and depending on the risk and level of exposure***, take ~~proactive~~ ***proportionate specific*** measures to protect their services against the dissemination of terrorist content ***that fully respect the fundamental rights of the users, and the fundamental importance of the freedom of expression and information as well as the right to privacy and protection of personal data in an open and democratic society. Such measures may include systems to allow users to report potential terrorist content or peer-to-peer content moderation. Such measures shall be taken in accordance with Article 3(1) and in particular shall not include automated content filters or other measures that entail the systematic monitoring of user behaviour.*** ~~The measures shall~~ ***They shall*** be ~~effective~~ ***targeted*** and proportionate, taking into account the risk and level of exposure to terrorist content, ***and must respect the constitutional arrangements of the Member State in which the main establishment of the hosting service provider or its designated representative is located***. ~~the fundamental rights of the users, and the fundamental~~

~~importance of the freedom of expression and information in an open and democratic society~~. ***This paragraph is without prejudice to possible additional voluntary measures taken by the hosting service provider outside the scope of this Regulation.***

2. Where it has been informed according to Article 4(9), the competent authority ***of the Member State in which the main establishment of the hosting service provider or its designated representative is located*** referred to in Article 17(1)(c) shall request the hosting service provider to submit a report, within ~~three~~ ***six*** 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~~ ***specific*** measures are ~~effective~~ ***targeted*** and proportionate, ~~including~~ ~~to evaluate~~ ~~the functioning of any~~ ***and*** ~~automated tools used~~ ***whether*** the ***specific measures are based on*** human oversight and ***whether effective*** ~~verification~~ mechanisms ***to protect users' fundamental rights are*** employed.

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

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

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

**CA 8 covering Article 7**
**Replacing all relevant amendments, including: Rapp 63, EPP 317, S&D 319**

*Article 7*
*Preservation of content and related data*

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

   (a) proceedings of administrative or judicial review,

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

   ***(c) remedying complaints following the mechanism described in Article 10.***

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

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

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

**CA 9 covering Article 8**
**Replacing all relevant amendments, including: Rapp 68, Rapp 69, Rapp 71, Rapp 73 S&D 322, ECR 324, S&D 325, EPP 326, ECR 327, EPP 328, GUE 329, EPP 330, EPP 331, ECR 333, EPP 334**

1. Hosting service providers shall ~~set out~~ ***explain in a clear manner*** in their terms and conditions their policy ~~to prevent the dissemination of~~, ***with regard to*** terrorist content ***and protection of users from such content***, including, ~~where appropriate~~, a meaningful explanation of the functioning of ~~proactive~~ ***specific*** measures***, as well as any additional voluntary measures a hosting service provider may employ in addition to its obligations under this Regulation, including*** the use of automated tools ***where applicable, as well as a description*** of the ***complaint mechanism available for content providers in accordance with Article 10***.

2. Hosting service providers, ***unless there has been no specific action required by them under this Regulation in any given year,*** and ***competent authorities and relevant***

***Union bodies*** shall ~~publish~~ ***make publicly available*** annual transparency reports on action taken against the dissemination of terrorist content.

3. Transparency reports ***of hosting service providers*** shall include at least the following information:

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

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

(c) number of pieces of terrorist content removed or to which access has been disabled, following removal orders, referrals, or ~~proactive~~ ***specific measures pursuant to this Regulation, as well as voluntary measures***, respectively;

(d) overview and outcome of complaint procedures ***including the number of cases in which it was established that content was wrongly identified as terrorist content***.

***(da) Transparency reports of competent authorities and relevant Union bodies shall include information on the number of removal orders and referrals issued, including information on the number of removals that led to successful detection, investigation and prosecution of terrorist offences, and on their use of the terrorist content, which has been preserved pursuant to Article 7 for the prevention, detection, investigation and prosecution of terrorist offences.***

**CA 10 covering Article 8a (new)**

**Replacing all relevant amendments, including: S&D 273, Rapp 335, S&D 345, ECR 346, ECR 349, ALDE 362**

***Article 8a***
***Appeal and redress***

***Member States shall ensure that a content provider or a hosting service provider can appeal a removal order as referred to in Article 4(9) by seeking redress in front of the relevant judicial authority in the Member State in which the content provider is located or in which the main establishment of the hosting service provider or legal representative designated by the hosting service provider pursuant to Article 16 resides or is established.***

**CA 11 covering Article 9**

**Replacing all relevant amendments, including: Rap 74, Rapp 76, ALDE 336, S&D 337, ALDE 339, Rapp 77, ECR 340, GUE 341**

*Article 9*

*Safeguards regarding ~~the use and implementation of proactive measures~~* ***content removal***

1. Where hosting service providers use ~~automated tools~~ voluntary measures pursuant to ***or measures otherwise in pursuit of the aims of*** this Regulation in respect of content that they store, they shall provide effective and appropriate safeguards to ensure that decisions taken concerning that content, in particular decisions to remove or disable content considered to be terrorist content, are accurate and well-founded ***, and do not lead to the removal or disabling of access to content that is not terrorist content***.

2. Safeguards shall consist, in particular, of human oversight and verifications ~~where appropriate and, in any event~~ ***of the appropriateness of the decision to remove or disable access to content, in particular with regard to the right to freedom of expression and information.***~~, 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~~.

**CA 12 covering Article 10**

**Replacing all relevant amendments, including: Rapporteur 75, Rapp 78, Rapp 335, S&D 345, ECR 346, EPP 342, GUE 343, ECR 344**

***-1. Content providers, whose content has been removed or access to it has been disabled, shall have the right to an effective remedy in accordance with Article 19 TEU and Article 47 of the Charter of Fundamental rights of the European Union.***

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 removal order pursuant to Article 4,*** a referral pursuant to Article 5***,*** ~~or of~~ ***specific*** ~~proactive voluntary~~ measures pursuant to ~~as referred to in~~ ***Article 6 or of additional voluntary measures***, to submit a complaint against the action of the hosting service provider requesting reinstatement of the content. ***Safeguards relating to removal or disabling of access shall also include the possibility of judicial redress***.

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 ***without undue delay and no later than two weeks from the receipt of the complaint, unless national law provides for a different deadline***.

**CA 13 covering Article 11**

**Replacing all relevant amendments, including: Rapp 347, ECR 348, Rapp 80**

1. Where hosting service providers remove terrorist content or disable access to it, they shall make available to the content provider ***comprehensive*** information on the removal or disabling of access to terrorist content ***provided to them by the competent authority in line with Article 4(3), including the legal basis establishing that it is terrorist content and possibilities to contest the decision including formal requirements, the description of the next steps of the procedure and related timeframes.***

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

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

**CA 14 covering Article 17**

**Replacing all relevant amendments, including: Rapp 88, Rapp 89, Rapp 90, EPP 364, S&D 365, ECR 366, GUE 367**

1. Each Member State shall designate ~~the~~ ***a single*** authority ~~or authorities~~ ***for the purpose of implementing this Regulation unless their constitutional arrangements prevent a single authority from being responsible. That authority shall be*** competent to:

   (a) issue removal orders pursuant to Article 4***, subject to independent judicial review in the case of administrative authorities***;

   (b) detect, identify and refer ***potential*** terrorist content to hosting service providers pursuant to Article 5 ***while the assessment of whether it meets the definition of terrorist content is pending***;

   (c) oversee the implementation of ~~proactive~~ ***specific*** measures pursuant to Article 6 ***as well as voluntary measures referred to in Article 9***;

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

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

**CA 15 covering Article 18**
**Replacing all relevant amendments, including: Rapp 91, Rapp 94, S&D 368, GUE 369, S&D 374, EPP 375, GUE 376, EPP 377, S&D 387, S&D 388, S&D 389, S&D 390, ECR 391**

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

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

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

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

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

   (e) Article 7 (preservation of data);

   (f) Article 8 (transparency);

   (g) Article 9 (safeguards in relation to ~~practive measures~~ ***content removal***);

   (h) Article 10 (complaint procedures);

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

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

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

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

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

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

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

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

   (c) previous breaches by the legal person held responsible***, a subsidiary or linked person or undertaking***;

(d) the financial strength of the legal person held liable***, a subsidiary or linked person or undertaking***;

(e) the level of cooperation of the hosting service provider ***or their representatives*** with the competent authorities.

***(f) unintentional delays, in particular by small and medium sized businesses and start-ups.***

4. Member States shall ensure that a systematic failure to comply with obligations pursuant to Article 4(2) is subject to financial penalties of ***at least 1% and*** up to 4% of the hosting service provider's global turnover of the last business year.

**CA 16 covering Annex I: paragraph 1, Section B and Section G**
**Replacing all relevant amendments, including: Rapp 398, EPP 399, Rapp 400, EPP 401, Rapp 402, Rapp 403**

Under Article 4 of Regulation (EU)….[16] the addressee of the removal order shall remove terrorist content or disable access to it, within ***the deadline specified by*** the competent authority.

In accordance with Article 7 of Regulation (EU) …. , addressees must preserve content and related data, which has been removed or access to it disabled, for six months or longer upon request from the competent authorities or courts ***or the content provider in order to remedy complaints following the mechanism described in Article 10***.

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

SECTION B: Content to be removed or access to it disabled within ~~one hour~~ ***the deadline specified by the competent authority***:
A URL and any additional information ***including screenshot where obtainable*** enabling the identification and exact location of the content referred:
……
Reason(s) explaining why the content is considered terrorist content, in accordance with Article 2 (5) of the Regulation (EU) xxx. The content (tick the relevant box(es)):
□ incites, advocates or glorifies the commission of terrorist offences (Article 2 (5) a)
□ encourages the contribution to terrorist offences (Article 2 (5) b)
□ promotes the activities of a terrorist group, encouraging participation in or support of the group (Article 2 (5) c)
□ provides instructions or techniques for committing terrorist offences (Article 2 (5) d)

Additional information on the reasons why the content is considered terrorist content (~~optional~~***) in accordance with national law, possibilities to contest the decision including formal requirements, the description of the next steps of the procedure and related timeframes***:

SECTION G: Information about redress possibilities
Information about competent body or court, deadlines and procedures ***including formal requirements*** for contesting the removal order:
Competent body or court to contest the removal order:
……
Deadline for contesting the decision:
Xxx months starting from xxxx

Link to provisions in national legislation:

RECITALS

**CA A covering recitals 1, 1a (new), 3, 4, 5, 6, 7, 7a (new), 7b (new) and 8 (relating to Article 1)**

**Replacing all relevant amendments, including: Rapp 2-9, EPP 98, S&D 99, ECR 104, EPP 105, ALDE 106, S&D 108, GUE 109, ALDE 111, EPP 112, S&D 113, GUE 114, EPP 115, ALDE 116, ECR 117, S&D 118, ALDE 119-120, ECR 121, S&D 122, ALDE 123**

(1) This Regulation aims at ensuring the smooth functioning of the digital single market in an open and democratic society, by ~~preventing~~ ***addressing*** the misuse of hosting services for terrorist purposes. 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***, the right to freedom and pluralism of the media, the freedom to conduct a business and the rights to privacy and protection of personal data***.

***(1a) Regulation of hosting service providers can only complement Member States' strategies to address terrorism, which must emphasise offline measures such as investment in social work, de-radicalisation initiatives and engagement with affected communities to achieve a sustainable prevention of radicalisation in society.***

(3) The presence of terrorist content online has serious negative consequences for users, for citizens and society at large as well as for the online service providers hosting such content, since it undermines the trust of their users and damages their business models. In light of their central role and ***in proportion to*** 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 ***competent authorities to*** tackle terrorist ~~content disseminated~~ ***offences committed*** through their services, ***whilst taking into account the fundamental importance of the freedom of expression and information in an open and democratic society***.

(4) Efforts at Union level to counter terrorist content online commenced in 2015 through a framework of voluntary cooperation between Member States and hosting service providers need to be ~~complemented by~~ ***improved through*** a clear legislative framework in order to further reduce accessibility to terrorist content online ~~and adequately address a rapidly evolving problem~~ ***and in order to put in place urgently needed safeguards to ensure the rule of law and the protection of fundamental rights***. This legislative framework seeks to build on voluntary efforts, which were reinforced by the Commission Recommendation (EU) 2018/334[1] and responds to calls made by the European Parliament to strengthen measures to tackle illegal and harmful content ***in line with the horizontal framework established by Directive 2000/31/EC*** and by the European Council to improve the ~~automatic~~ detection and removal of content that incites to terrorist acts.

(5) ***This Regulation should lay down specific obligations for hosting service providers, exposed to terrorist content.*** ~~The application of this~~ ***This*** Regulation should not affect

[1] 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).

the application of ~~Article 14 of~~ Directive 2000/31/EC[2]. ~~In particular, any measures taken by the hosting service provider in compliance with this Regulation, including any proactive measures, should not in themselves lead to that service provider losing the benefit of the liability exemption provided for in that provision.~~. This Regulation leaves unaffected the powers of national authorities and courts to establish liability of hosting service providers in specific cases where the conditions under ~~Article 14~~ of Directive 2000/31/EC for liability exemption are not met.

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

(7) This Regulation ~~contributes~~ ***aims at contributing*** 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, ***the rights to privacy and to personal data protection as well as the freedom of the press and pluralism of the media,*** which constitute~~s~~ ~~one of~~ the essential foundations of a pluralist, democratic society, and ~~is one of~~ ***are among*** the values on which the Union is founded. Measures ***taken to remove terrorist content online should avoid any*** ~~constituting~~ interference in the freedom of expression and information ***and*** should be strictly targeted~~, in the sense that they must serve to prevent the dissemination terrorist content~~ ***necessary, appropriate and proportionate to help the fight against terrorism, including investigation and prosecution of terrorist offences***, but without thereby affecting ***freedom of expression,*** 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.

***(7a) This Regulation should not have the effect of modifying the obligation for Member States to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on the European Union. Those fundamental rights include the freedom to hold opinions and to receive and impart information and ideas without interference by public authorities. Any restrictions to the exercise of these fundamental rights within the framework of this Regulation should be prescribed by law and should be necessary in a democratic society, with the aim of fulfilling the aims of this Regulation.***

***(7b) This Regulation should respect the fundamental rights and observe the principles recognised in the European Convention on Human Rights and in the case-law of the European Court of Justice. In particular, in its judgment of 24 November 2011 the European Court of Justice concluded that Union law, and in particular Directive***

[2] 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).

***2000/31/EC[3] and the applicable fundamental rights, precluded an injunction imposed on an Internet service provider to introduce a system for filtering all electronic communications passing via its services, applied indiscriminately to all its customers, as a preventive measure, exclusively at its expense and for an unlimited period.***

(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 right for the hosting service providers and content providers to be informed about all available means of redress and the possibility for content providers to contest the results of measures taken by the hosting provider, and to be informed of effective means of remedies. It also includes the right*** ~~the possibility~~ for hosting service providers and content providers to effectively contest the removal orders ***or penalties*** before the court of the Member State whose authorities issued the removal order ***or penalties, or the court where the hosting service provider or content provider is established or represented***.

**CA B covering recitals 9 and 10 (relating to Article 2)**
**Replacing all relevant amendments, including: Rapp 10-11, ALDE 124, S&D 125, EPP 126, ECR 127, EPP 129, GUE 130, EPP 131, ALDE 132, S&D 133, ECR 134, EPP 135**

(9) In order to provide clarity about the actions that both hosting service providers and ***the*** competent ~~authorities~~ ***authority*** should take to ~~prevent~~ ***restrict*** the dissemination of terrorist content online, this Regulation should establish a definition of terrorist content ~~for preventative purposes drawing on~~ ***in line with*** the definition of terrorist offences under Directive (EU) 2017/541 of the European Parliament and of the Council[4]. Given the need to address ~~the most harmful~~ terrorist propaganda online, the definition should capture material and information that ***intentionally*** incites~~, encourages~~ or advocates the commission ~~or contribution to~~ ***of*** terrorist offences, ***or intentionally*** provides instructions for ***the making and use of explosives, firearms or other weapons or noxious or hazardous substances for the purpose of*** the commission of such offences***, knowing that the skills provided are intended to be used for this purpose,*** or ~~promotes the participation~~ ***participates*** in activities of a terrorist group. Such information includes in particular text, images, sound recordings and videos. When assessing whether content constitutes terrorist content within the meaning of this Regulation, competent authorities ~~as well as hosting service providers~~ should take into account factors such as the nature and wording of the statements, the context in which the statements were made***, their intentionality*** and their potential to lead to harmful consequences, thereby affecting the security and safety of persons. The fact that the ~~material~~ ***offences or content were***~~was~~ produced by, ~~is~~ ***are*** attributable to or disseminated on behalf of an EU-listed terrorist organisation or person constitutes an important factor in the assessment. Content

[3] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

[4] 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).

disseminated for educational, ***counter-narrative***, journalistic or research purposes should be ~~adequately~~ ***strongly*** protected. ***Where the disseminated material is published under the editorial responsibility of the hosting provider, any decision as to the removal of such content should take into account the journalistic standards established by press or media regulation consistent with the law of the Union and the right to freedom of expression and the right to freedom and pluralism of the media as enshrined in Article 11 of the Charter of Fundamental Rights***. Furthermore, the expression of radical, polemic or controversial views in the public debate on sensitive political questions should not be considered terrorist content. ***The right to such expression can be invoked before the court of the Member State where the hosting service provider has its main establishment or where the legal representative designated by the hosting service provider pursuant to this Regulation resides or is established, as well as the court of the Member State where the content provider is based.***

(10) In order to cover those online hosting services where terrorist content is disseminated, this Regulation should apply ***to the extent that it is possible to identify and remove specific content that is the subject of this Regulation,*** 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 ***directly*** available to ***the public*** ~~third parties, irrespective of whether this activity is of a mere technical, automatic and passive nature~~. ***The definition of hosting service providers is therefore distinct from and narrower than that employed in Directive 2000/31/EC***. 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 ***publicly*** available ~~to third parties and websites where users can make comments or post reviews~~***and accelerate the dissemination of content***. ***Providers of services such as online encyclopaedias, educational and scientific repositories, open source software developing platforms, cloud infrastructure service providers and cloud providers (including business-to-business cloud services), should not be considered hosting service providers within the meaning of this Regulation***. ***Mere conduits and other electronic communication services within the meaning of Directive (EU) 2018/1972 or providers of caching services, or other services provided in other layers of the Internet infrastructure, such as registries and registrars, DNS (domain name system) or adjacent services, such as payment services or DDoS (distributed denial of service) protection services are excluded from the scope.*** 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.

**CA C covering recital 12 (relating to Article 3)**
**Replacing all relevant amendments, including: Rapp 12, GUE 136**

(12) Hosting service providers ***exposed to terrorist content*** should apply certain duties of care, in order to ~~prevent~~ ***restrict*** the dissemination of terrorist content on their services. These duties of care should not amount to a general ~~monitoring~~ obligation ***on hosting service providers to monitor the information which they store, nor to a general obligation to actively seek facts or circumstances indicating illegal activity***. Duties of care should include that, when applying this Regulation, hosting services providers act in a ***transparent,*** diligent, proportionate and non-discriminatory manner in respect of content that they store, in particular when implementing their own terms and conditions, with a view to avoiding removal of content which is not terrorist. The removal or disabling of access has to be undertaken in the observance of freedom of expression and information ***and freedom and pluralism of the media***.

**CA D covering recitals 13 and 13a (new) (relating to Article 4)**
**Replacing all relevant amendments, including: Rapp 13, S&D 137, ALDE 138, GUE 139, EPP 140, ECR 143, ALDE 144**

(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~~ ***freely designate a single*** competent ~~authorities~~ ***authority*** ~~allowing them to designate administrative, law enforcement or judicial authorities~~ with that task, unless ***their constitutional arrangements prevent a single authority from being responsible, whilst at the same time guaranteeing legal certainty and predictability to users and service providers***. ***Where the authority designated for issuing removal orders is of an administrative or law enforcement nature, the Member State should provide for an effective and independent review of removal orders issued by the competent authorities in its Member State. This review would provide a mechanism to assess ex officio (in the absence of a request for review) individual removal orders and rectify any erroneous decisions. This review mechanism complements possibilities for hosting service providers and content providers to seek judicial redress against removal orders addressed to or affecting them.*** ~~Given the speed at which terrorist content is disseminated across online services, this~~ ***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 ***the period specified by the competent authority*** ~~one hour from receiving the removal order~~***. The competent authority should provide the hosting service provider with a defined time limit in the removal order, which should be no shorter than 8 hours, taking into account the size and previous exposure to terrorist content of a hosting service provider***. ***Without prejudice to the requirement to preserve data under Article 7 of this Regulation, it*** ~~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.

***(13a) The removal order should include a classification of the relevant content as terrorist content and contain sufficient information so as to locate the content, by providing a URL and any other additional information, such as a screenshot, where obtainable, of the content in question. The competent authority should also provide a***

***supplementary statement of reasons as to why the content is considered terrorist content. The reasons provided need not contain sensitive information, which could jeopardise investigations. The statement of reasons should however allow the hosting service provider and, ultimately, the content provider to effectively exercise their right to judicial redress***.

**CA E, covering recital 15 (relating to Article 5)**
**Replacing all relevant amendments, including: Rapp 14**

(15) Referrals by the competent authorities or Europol constitute an effective and swift means of making hosting service providers aware of specific content on their services. This mechanism of alerting hosting service providers to information that may be considered terrorist content, for the provider's voluntary consideration of the compatibility its own terms and conditions ***as foreseen by Regulation (EU) 2016/794***, should remain available in addition to removal orders ***provided that the competent authority of the Member State in which the hosting service provider is establishedverifies swiftly after a referral has been issued whether the content subject to the referral constitutes terrorist content and follows it up by a removal order where appropriate***. It is important that ***the competent authorities or Europol provide a detailed assessment and*** 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~~ ***subject to a referral*** remains with the hosting service provider, ***unless it gets followed up by a removal order***.~~-~~In implementing this Regulation related to referrals, Europol's mandate as laid down in Regulation (EU) 2016/794[5] remains unaffected.

**CA F, covering recitals 16, 17, 18 19 and 19a (new) (relating to Article 6)**
**Replacing all relevant amendments, including: Rapp 15-18, GUE 149, EPP 150, ALDE 151, S&D 152, EPP 153, ALDE 154, GUE 155, ALDE 156, ECR 157, ECR 158, S&D 159, EPP 160**

(16) Given the ~~scale and speed necessary for~~ ***complexity of*** effectively identifying and removing terrorist content ***at scale and the potential impact on fundamental rights***, proportionate ~~proactive~~ ***specific*** measures~~, including by using automated means in certain cases~~ ~~are an essential element in tackling~~ ***should be taken by hosting service providers depending on the risk and level of exposure***, ***concerning*** terrorist content online. ***Such obligatory measures should not include the use of content filters or other measures that entail the systematic monitoring of user behaviour. Specific measures could include, for example, systems to allow users to report potential terrorist content or peer-to-peer content moderation.*** With a view to reducing the

[5] 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).

accessibility of terrorist content on their services, hosting service providers should assess whether it is appropriate to take ~~proactive~~ ***specific*** 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 ***justified,*** appropriate, effective and proportionate ~~proactive~~ ***specific*** 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~~ . ***This is without prejudice to possible additional voluntary measures taken by the hosting service provider outside the scope of this Regulation.***

(17) When putting in place ~~proactive~~ ***specific*** measures, hosting service providers should ensure that users' ~~right~~ ***rights*** to freedom of expression and information - including to freely receive and impart information - ***as well as the right to privacy and personal data protection*** 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***, as well as including*** ~~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~~***measures against terrorist content, including voluntary ones,, whether taken by the hosting service provider itself or pursuant to a request by the competent authority,*** should be assessed with regard to the reliability of the underlying technology and the ensuing impact on fundamental rights. ***In any case, hosting service providers should undertake a fundamental rights audit for any voluntary or specific measures they use.***

(18) In order to ensure that hosting service providers exposed to terrorist content take appropriate ***specific*** measures to ~~prevent the misuse of~~***protect*** their services ***against misuse***, the competent authorities should request hosting service providers having received a removal order, which has become final, to report on ~~the~~ ***any specific*** ~~proactive~~ measures taken***, where applicable***. ~~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 ***necessary,*** effective and proportionate and whether, ~~if automated means are used,~~ the ~~hosting service provider has the necessary abilities for~~***specific measures are based on*** 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 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) ***as well as the safeguards put in place to protect freedom of expression and information and the number of incidents of restrictions on legal content***.

(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.~~

***(19a) A hosting service provider should be able, at any time, to request the competent authority to review and, where appropriate, to revoke a request pursuant to Article 6(2). The competent authority should provide a reasoned decision within a reasonable period of time after receiving the request by the hosting service provider.***

**<u>CA G covering recitals 24, 24a (new), 25 and 26 (relating to Article 8)</u>**
**Replacing all relevant amendments, including: Rapp 20, Dalton 162, Rapp 21, ALDE 164, S&D 165, ECR 166, Rap 22, EPP 167, ECR 168**

(24) Transparency of hosting service providers' policies in relation to terrorist content is essential to enhance their accountability towards their users and to reinforce trust of citizens in the Digital Single Market. Hosting service providers ***exposed to illegal terrorist content*** should publish annual transparency reports containing meaningful information about action taken in relation to the detection, identification and removal of terrorist content ***including voluntary measures as well as the number of contested removals***. ***Hosting service providers should not be required to disclose any source code as part of their transparency reports***. ***Competent authorities should also publish annual transparency reports containing meaningful information on the number of removal orders issued, the number of removals, the number of identified and detected terrorist content removed and the number of contested removals.***

***(24a) Content providers whose content has been removed should have a right to an effective remedy in accordance with Article 19 TEU and Article 47 of the Charter of Fundamental rights of the European Union. Certain hosting providers already use automated tools in order to remove illegal content from their platforms. Such technologies are unable to differentiate illegal terrorist content from content that is legal, such as content that is disseminated for educational, journalistic or research purposes.***

(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 ***and this should include information on all effective remedy options, including judicial redress***. ***Content providers should also have the right to complain directly to the competent authority in their own Member State if they are unable to resolve their complaint with a hosting service provider.*** The requirement for the hosting

service provider to reinstate the content where it has been removed in error, does not affect the possibility of hosting service providers to enforce their own terms and conditions on other grounds.

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

**CA H covering recital 37 (relating to Article 17)**
**Replacing all relevant amendments, including: Rapp 30, ECR 143**

(37) For the purposes of this Regulation, Member States should designate ***a single*** competent ~~authorities~~ ***authority unless their constitutional arrangements prevent a single authority from being responsible***. The requirement to designate competent authorities does not necessarily require the establishment of new authorities but can be existing bodies tasked with the functions set out in this Regulation. This Regulation requires designating authorities competent for issuing removal orders, ~~referrals and for overseeing proactive measures~~ and for imposing penalties. ~~It is for Member States to decide how many authorities they wish to designate for these tasks~~**.**

**CA I covering recital 38 (relating to Article 18)**

**Replacing all relevant amendments, including: Rapp 31, ALDE 175, S&D 176, EPP 177, EPP 178, GUE 179, EPP 180**

(38) Penalties are necessary to ensure the effective implementation by hosting service providers of the obligations pursuant to this Regulation, ***and should also take into account the situation of subsidiaries or linked undertakings where applicable***. Member States should adopt rules on penalties, including, where appropriate, fining guidelines. ~~Particularly severe penalties shall~~ ***Penalties should*** be ascertained in the event that the hosting service provider systematically fails to remove terrorist content or disable access to it within ~~one hour from receipt of a removal order~~ ***the period specified by the competent authority***. ~~Non-compliance in individual cases could be sanctioned while respecting the principles of *ne bis in idem and of* proportionality and ensuring that such sanctions take account of systematic failure. In order to ensure legal certainty, the~~

~~regulation should set out to what extent the relevant obligations can be subject to penalties. Penalties for non-compliance with Article 6 should only be adopted in relation to obligations arising from a request to report pursuant to Article 6(2) or a decision imposing additional proactive measures pursuant to Article 6(4).~~ When ***assessing the nature of the breach and deciding upon applying penalties, full respect should be given to fundamental rights, such as the freedom of expression.*** When determining whether or not financial penalties should be imposed, due account should be taken of the financial resources of the provider, ***unintentional delays, in particular by small and medium sized businesses and start-ups***. Member States ~~shall~~ ***should*** ensure that penalties do not encourage the removal of content which is not terrorist content.